03 UPORABNA INFORMATIKA

2024 ‹ ŠTEVILKA 3 ‹ LETNIK XXXII ‹ ISSN 1318-1882

U P O R A B N A
I N F O R M A T I K A
2024 ŠTEVILKA 3 JUL/AVG/SEP LETNIK XXXII ISSN 1318-1882

Znanstveni prispevki

Strokovni prispevki

Pregledni znanstveni prispevki

Informacije

2024 ŠTEVILKA 3 JUL/AVG/SEP LETNIK XXXII ISSN 1318-1882

Ustanovitelj in izdajatelj
Slovensko društvo INFORMATIKA
Litostrojska cesta 54, 1000 Ljubljana

Predstavnik
Slavko Žitnik

Odgovorni urednik
Mirjana Kljajić Borštnar

Prelom in tisk
Boex DTP, d. o. o., Ljubljana

Naklada
110 izvodov

Naslov uredništva
Slovensko društvo INFORMATIKA
Uredništvo revije Uporabna informatika
Litostrojska cesta 54, 1000 Ljubljana
www.uporabna-informatika.si

Revija izhaja četrtletno. Cena posamezne številke je 20,00 EUR. Letna naročnina za podjetja 85,00 EUR, za vsak nadaljnji izvod 60,00 EUR, za posameznike 35,00 EUR, za študente in seniorje 15,00 EUR. V ceno je vključen DDV.

Revija Uporabna informatika je od številke 4/VII vključena v mednarodno bazo INSPEC.

Revija Uporabna informatika je pod zaporedno številko 666 vpisana v razvid medijev, ki ga vodi Ministrstvo za kulturo RS.

Revija Uporabna informatika je vključena v Digitalno knjižnico Slovenije (dLib.si).

Izid publikacije je finančno podprla Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije.

Vabilo avtorjem

V reviji Uporabna informatika objavljamo kakovostne izvirne prispevke domačih in tujih avtorjev z najširšega področja informatike, ki se nanašajo tako na poslovanje podjetij, javno upravo, družbo in posameznika. Prispevki so lahko znanstvene, strokovne ali informativne narave, še posebno spodbujamo objavo interdisciplinarnih prispevkov. Zato vabimo avtorje, da prispevke, ki ustrezajo omenjenim usmeritvam, pošljejo uredništvu revije po elektronski pošti na naslov ui@drustvo-informatika.si.

Avtorje prosimo, da pri pripravi prispevka upoštevajo navodila, ki so objavljena na naslovu http://www.uporabna-informatika.si.

Za kakovost prispevkov skrbi mednarodni uredniški odbor. Prispevki so anonimno recenzirani, o objavi pa na podlagi recenzij samostojno odloča uredniški odbor. Recenzenti lahko zahtevajo, da avtorji besedilo spremenijo v skladu s priporočili in da popravljeni prispevek ponovno prejmejo v pregled. Sprejeti prispevki so pred izidom revije objavljeni na spletni strani revije (predobjava), še prej pa končno verzijo prispevka avtorji dobijo v pregled in potrditev. Uredništvo lahko še pred recenzijo zavrne objavo prispevka, če njegova vsebina ne ustreza vsebinski usmeritvi revije ali če prispevek ne ustreza kriterijem za objavo v reviji.

Pred objavo prispevka mora avtor podpisati izjavo o avtorstvu, s katero potrjuje originalnost prispevka in dovoljuje prenos materialnih avtorskih pravic. Avtorji prejmejo enoletno naročnino na revijo Uporabna informatika, ki vključuje avtorski izvod revije in še nadaljnje tri zaporedne številke. S svojim prispevkom v reviji Uporabna informatika boste pomagali k širjenju znanja na področju informatike. Želimo si čim več prispevkov z raznoliko in zanimivo tematiko in se jih že vnaprej veselimo

Uredništvo revije

Navodila avtorjem člankov

Članke objavljamo praviloma v slovenščini, članke tujih avtorjev pa v angleščini. Besedilo naj bo jezikovno skrbno pripravljeno. Priporočamo zmernost pri uporabi tujk in, kjer je mogoče, njihovo zamenjavo s slovenskimi izrazi. V pomoč pri iskanju slovenskih ustreznic priporočamo uporabo spletnega terminološkega slovarja Slovenskega društva Informatika, Islovar (www.islovar.org).

Znanstveni prispevek naj obsega največ 40.000 znakov, kratki znanstveni prispevek do 10.000 znakov, strokovni članki do 30.000 znakov, obvestila in poročila pa do 8.000 znakov.

Prispevek naj bo predložen v urejevalniku besedil Word (*.doc ali *.docx) v enojnem razmaku, brez posebnih znakov ali poudarjenih črk. Za ločilom na koncu stavka napravite samo en presledek, pri odstavkih ne uporabljajte zamika.

Naslovu prispevka naj sledi polno ime vsakega avtorja, ustanova, v kateri je zaposlen, naslov in elektronski naslov. Sledi naj povzetek v slovenščini v obsegu 8 do 10 vrstic in seznam od 5 do 8 ključnih besed, ki najbolje opredeljujejo vsebinski okvir prispevka. Sledi naj prevod naslova povzetka in ključnih besed v angleškem jeziku. V primeru, da oddajate prispevek v angleškem jeziku, velja obratno. Razdelki naj bodo naslovljeni in oštevilčeni z arabskimi številkami.

Slike in tabele vključite v besedilo. Opremite jih z naslovom in oštevilčite z arabskimi številkami. Na vsako sliko in tabelo se morate v besedilu prispevka sklicevati in jo pojasniti. Če v prispevku uporabljate slike ali tabele drugih avtorjev, navedite vir pod sliko oz. tabelo. Revijo tiskamo v črno-beli tehniki, zato barvne slike ali fotografije kot original niso primerne. Slikam zaslonov se v prispevku izogibajte, razen če so nujno potrebne za razumevanje besedila. Slike, grafikoni, organizacijske sheme ipd. naj imajo belo podlago. Enačbe oštevilčite v oklepajih desno od enačbe.

V besedilu se sklicujte na navedeno literaturo skladno s pravili sistema IEEE navajanja bibliografskih referenc, v besedilu to pomeni zaporedna številka navajenega vira v oglatem oklepaju (npr. [1]). Na koncu prispevka navedite samo v prispevku uporabljeno literaturo in vire v enotnem seznamu, urejeno po zaporedni številki vira, prav tako v skladu s pravili IEEE. Več o sistemu IEEE, katerega uporabo omogoča tudi urejevalnik besedil Word 2007, najdete na strani https://owl.purdue.edu/owl/research_and_citation/ieee_style/ieee_general_format.html.

Prispevku dodajte kratek življenjepis vsakega avtorja v obsegu do 8 vrstic, v katerem poudarite predvsem strokovne dosežke.

Avtomatizacija kategoriziranja obstoječih učinkov uporabe odprtih podatkov glede na opise primerov uporabe

Nejc Čelik, Aljaž Ferencek
Univerza v Mariboru, Fakulteta za organizacijske vede
nejc.celik1@um.si, aljaz.ferencek1@student.um.si

Izvleček

Odprti podatki (OP) predstavljajo pomemben vir javno dostopnih podatkov, ki izhajajo iz javnega sektorja. Osrednji cilj OP je omogočanje transparentnosti, odgovornosti in ustvarjanje dodane vrednosti. Z naraščanjem količine podatkov, ki jih ustvarja javni sektor, rastejo tudi prizadevanja za zagotavljanje njihove dostopnosti javnosti. Raziskave kažejo, da so OP dostopni javnosti in tudi uporabljeni na področju ekonomije, kjer podjetja uporabljajo poslovno inteligenco v kompleksnem globalnem gospodarstvu. Vendar pa ekonomske koristi predstavljajo le en vidik učinka OP. Prepoznavanje in kvantificiranje učinka OP je oteženo zaradi njegove posredne narave. Študije, ki prepoznavajo učinek OP, obsegajo predhodne ocene iz anket, ki so omejene s strani osebja in financiranja za dejavnosti, povezane z OP. Izziv torej leži v prepoznavanju učinkov OP, za kar v literaturi zasledimo predloge uporabe tehnik podatkovnega rudarjenja in umetne inteligence. Namen te raziskave je potrditi že prepoznana področja učinkov OP s strani Evropske komisije in usmeriti nadaljnje raziskave s predlogom novih področij učinkov. V raziskavi smo se ravnali po metodi CRISP-DM, uporabili pa smo različne modele strojnega učenja za klasifikacijo primerov uporabe OP. Rezultati kažejo na potencial umetne inteligence pri prepoznavanju učinkov OP, a je potrebno izdelati končno in podrobnejšo taksonomijo prepoznanih področij učinka. Raziskava je prepoznala nove kategorije uporabe OP, ki bi lahko prispevale k bolj natančni in uporabni klasifikaciji učinkov uporabe OP.

Ključne besede: odprti podatki, podatki javnega sektorja, umetna inteligenca, nevronske mreže

Automating the Categorization of Existing Open Data Impacts Based on Use Case Descriptions

Abstract

Open Government Data (OGD) represents an important source of publicly accessible data originating from the public sector. The primary goal of OGD is to enable transparency, accountability, and the creation of added value. With the increasing volume of data generated by the public sector, there is a strong effort to ensure its accessibility to the public. Research shows that OGD is accessible to the public and also used in the field of economics, where companies utilize business intelligence in a complex global economy. However, economic benefits represent only one of the aspects of the impact of OGD. Recognizing and quantifying the impact of OGD is challenging due to its indirect nature. Studies assessing the impact of OGD include preliminary estimates from surveys, which are limited by staff and funding for OGD-related activities. The challenge lies in recognizing the impact of OGD, for which the literature suggests using data mining and artificial intelligence techniques. The purpose of this research is to confirm the already recognized areas of OGD impact by the European Commission and to guide further research with the proposal of new impact areas. The research followed the CRISP-DM method and utilized various machine learning models to classify OGD use cases. The results indicate the potential of artificial intelligence in recognizing the impacts of OGD, however, there is a need to develop a final and more detailed taxonomy of identified impact areas. The research identified new categories of OGD use that could contribute to a more precise and useful classification of OGD impacts.

Keywords: open data, open government data, artificial intelligence, neural networks

1 UVOD

Odprti podatki (OP) predstavljajo pomemben vir javno dostopnih podatkov, ki izhajajo iz javnega sektorja. Osrednji cilj OP je omogočanje transparentnosti, odgovornosti in ustvarjanje dodane vrednosti [1]. V zadnjih letih smo priča znatnemu porastu produkcije in analize podatkov v javnem sektorju. Ta trend je privedel do občutnega povečanja raziskav na področju odprtih podatkov [2], [3], [4]. Z naraščanjem količine podatkov, ki jih ustvarja javni sektor, rastejo tudi prizadevanja za zagotavljanje njihove dostopnosti javnosti. Ta prizadevanja so skladna s širšim dolgoročnim ciljem, ki je izboljšanje splošne transparentnosti vlade [5], [6].

Iz literature je moč zaznati, da so OP dostopni javnosti in tudi uporabljeni, kot na primer na področju ekonomije, saj podjetja vse bolj izkoriščajo odprte podatke in uporabljajo metode poslovne inteligence za poslovanje v kompleksnem globalnem gospodarstvu [7]. Čeprav se ekonomske koristi morda lažje kvantificirajo, vseeno predstavljajo le en vidik prednosti, ki jih ponujajo OP [8]. Zapletenost prepoznavanja in kvantificiranja učinka OP je še dodatno otežena zaradi posredne narave koristi, ki jih OP prinašajo [9]. Poleg tega študije, ki ocenjujejo učinek OP, večinoma obsegajo predhodne ocene, pridobljene iz anket [10]. Medtem ko anketne ocene ponujajo koristne vpoglede, so rezultati ali njihova koristnost omejeni s strani osebja in financiranja za dejavnosti povezanimi z odprtimi podatki na strani vladnih služb, saj javni uslužbenci pogosto prevzemajo druge, bolj prioritetne projekte [11].

Izziv torej leži v prepoznavanju učinka odprtih podatkov, za reševanje katerega pa Ferencek in Kljajić Borštnar [12], [13], [14], [15] predlagata uporabo tehnik podatkovnega rudarjenja in umetne inteligence na primerih uporabe, ki so objavljeni s strani Urada za publikacije Evropske unije [16]. Njune raziskave zaenkrat kažejo na potencial uporabe tehnik umetne inteligence za prepoznavanje učinka OP, a je pred vsesplošno uporabo predlaganih pristopov potrebno izdelati taksonomijo prepoznanih področij OP, ki pa se lahko razlikuje ali sovpada s področji učinka, ki se v anketah članic Evropske Unije (EU) uporabljajo za izdelavo Ocene zrelosti odprtih podatkov [17]. Slednja se izvaja za merjenje napredka evropskih držav pri spodbujanju in omogočanju razpoložljivosti in ponovne uporabe informacij javnega sektorja, zajema pa štiri razsežnosti zrelosti odprtih podatkov: politike (stopnja razvoja nacionalnih politik), ki spodbujajo odprte podatke; portali (značilnosti in podatki, ki so na voljo na nacionalnih podatkovnih portalih); kakovost (metapodatkov na nacionalnih podatkovnih portalih) in učinki (pobude za spremljanje ponovne uporabe in učinka odprtih podatkov) [18]. Ker v tej raziskavi preučujemo učinek OP, smo se zato posebej osredotočili na razsežnost »učinki«, ki spremlja pobude za spremljanje ponovne uporabe in učinka odprtih podatkov. Omenjena razsežnost v Oceni zrelosti odprtih podatkov, glede na OECD (Organisation for Economic Co-operation and Development) [17] definira štiri glavna področja učinka, ki so družbeno (angl. social), okoljsko (angl. environmental), vladno (angl. governmental) in ekonomsko (angl. economic).

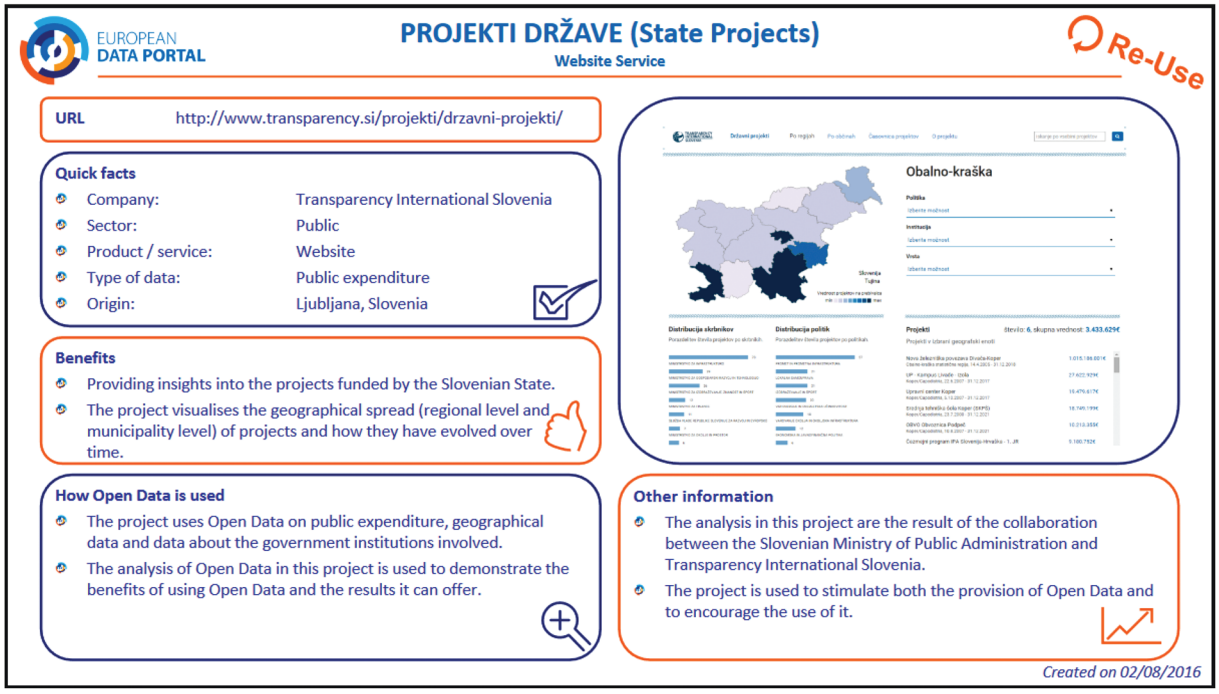
Namen te raziskave je torej potrditi že prepoznana in uveljavljena področja učinka OP s strani Evropske Komisije na podlagi podatkovne zbirke, ki jo uporabljata Ferencek in Kljajić Borštnar [13], [14] v svojih raziskavah za prepoznavo bolj podrobnih področij učinka in izdelavo taksonomije področij OP z metodami umetne inteligence. V prejšnjih raziskavah so bile za avtomatsko prepoznavanje področji učinkov uporabljene preprostejše metode, kot sta npr. TD-IDF [19] in Yake! [20], ki pa nista prinesli želenih rezultatov [14]. V tej raziskavi smo zato uporabili tudi model globoke nevronske mreže [21].

2 METODOLOGIJA

V prispevku naslavljamo problem razvoja klasifikacijskega problema za avtomatizirano določanje kategorije učinkov aplikacij odprtih podatkov.

Pri tem smo sledili metodologiji načrtovanja in razvoja (Design Science Research) [22], ki je sestavljena iz treh glavnih ciklov (opredelitev problema, razvoj in vrednotenje rezultatov). V ciklu razvoja smo uporabili CRISP-DM [23] za razvoj in evalvacijo modela za klasifikacijo učinkov aplikacij odprtih podatkov. CRISP-DM vključuje faze od poslovnega razumevanja, priprave in razumevanja podatkov, do modeliranja, evalvacije in implementacije. S kombinacijo teh pristopov smo sistematično zbirali in preprocesirali podatke, razvijali modele strojnega učenja ter jih iterativno izboljševali, kar je omogočilo robustno klasifikacijo učinkov aplikacij odprtih podatkov.

Ideja prispevka je, da lahko iz opisov primerov uporabe razvijemo model, s katerim bi lahko avtomatsko uvrstili primere uporabe odprtih podatkov glede na področje učinka uporabe.



Slika 1: **Zajeta slika PDF dokumenta enega od primerov uporabe [16], ki smo jih uporabili v tej raziskavi.**

Zbrali smo 697 opisov primerov uporabe, dostopnih na European data portal [16]. Ti opisi so shranjeni v PDF datotekah z osnovnimi podatki o primeru uporabe in krajšim opisom uporabe podatkov ter morebitnimi dodatnimi informacijami ali načrti za nadaljnji razvoj (Slika 1). V PDF datotekah je običajen tudi okvir, ki vsebuje sliko, ki občasno prikazuje izdelan produkt (npr. uporabniški vmesnik) pogosto pa je na sliki le logotip projekta, zato smo se odločili, da v okviru tega članka teh slik ne bomo uporabljali.

Za razvrstitev primerov uporabe v različne kategorije učinkov uporabe smo analizirali njihove opise. Domenski ekspert je razvrstil 697 primerov uporabe v eno od štirih kategorij učinkov (družbena, okoljska, vladna in ekonomska). Prepoznanih je bilo 421 družbenih, 94 okoljskih, 96 vladnih in 86 ekonomskih primerov uporabe (Tabela 1).

Tabela 1: **Tabelarični prikaz kategorij učinkov in pripadajoče število primerov uporabe.**

Kategorija primera uporabe	Število primerov uporabe
DRUŽBENI	421
OKOLJSKI	94
VLADNI	96
EKONOMSKI	86

Za klasifikacijo primerov uporabe smo najprej pretvorili besedila v vektorski prostor. Za pretvorbo smo uporabili več metod in sicer TF-IDF metodo [19] in model globoke nevronske mreže [21] s transformer arhitekturo [24]. Model nevronske mreže ki smo ga uporabili je imenovan General-purpose Text Embeddings v1.5 (GTE) [25], [26], ki je prilagojen BERT model [27] za vektorizacijo besedila. Za obe metodi smo uporabili surovo obliko besedila izluščenega iz pdf datotek in preprocesirano obliko besedila, kjer smo iz besedila ostranili »stop-words« besede, pretvorili besedilo v male črke, izvedli lematizacijo in odstranili razne šume, kot so ločila, posebni znaki, polni URL-ji, e-poštni naslovi, podvojeni presledki ipd.

Za lažje razumevanje podatkov smo dobljene vektorje vizualizirali s pomočjo tehnike UMAP [28]. UMAP (Uniform Manifold Approximation and Projection) je tehnika za zmanjšanje dimenzionalnosti podatkov, kar omogoča vizualizacijo večdimenzionalnih podatkov v dvo- ali tridimenzionalnem prostoru. Ta tehnika je še posebej uporabna za vizualizacijo kompleksnih podatkovnih nizov, kot so besedilni vektorji, saj omogoča enostavno prepoznavanje vzorcev in skupin.

Ker je bilo primerov uporabe v kategoriji »Družbeni« bistveno več kot v drugih kategorijah (421),

Tabela 2: **Tabelarični prikaz elementov hiperparametrizacije ter njihovih vrednosti**

Hiperparametri	Vrednost
Velikost paketa (ang. batch size)	32
Število epoh (ang. epoch)	10
Začetna stopnja učenja (ang. initial learning rate)	5e-4 (»cosine decay« [35] do 0 v korakih)
Naključno izpuščanje (ang. dropout) [29]	50 %
Skriti sloj	1024 nevronov (»GELU« aktivacijska funkcija [32])
Izhodni sloj	4 nevroni (»softmax« aktivacijska funkcija [33])

smo za uravnoteženje nabora podatkov pri klasifikaciji naključno izbrali 100 primerov uporabe iz te kategorije [29]. Preostale primere uporabe iz te kategorije smo odstranili iz nabora podatkov.

Uravnotežene podatke smo naključno razdelili na učno in testno množico v razmerju 66 % učni in 33 % testni. Za klasifikacijo v kategorije smo uporabili naslednje metode: nevronska mreža [21], naključni gozd (random forest) [30] in metoda podpornih vektorjev (Support Vector Machine - SVM) [31]. Velikost in globino naključnega gozda smo določili s testiranjem naključnih kombinacij, kjer smo globino variirali med 1 in 5, velikost pa med 10 in 500.

Nevronska mreža [29], ki smo jo uporabili za klasifikacijo, je sestavljena iz enega skritega sloja s 1024 nevroni z »GELU« [32] aktivacijsko funkcijo in izhodnim slojem z 4 nevroni s »softmax« [33] aktivacijsko funkcijo. Med vhodi in prvim (skritim) slojem ter med prvim in izhodnim slojem smo med učenjem uporabili naključno izpuščanje (ang. dropout) [34] z verjetnostjo 50 %. V tabeli (Tabela 2) so prikazani hiperparametri učenja.

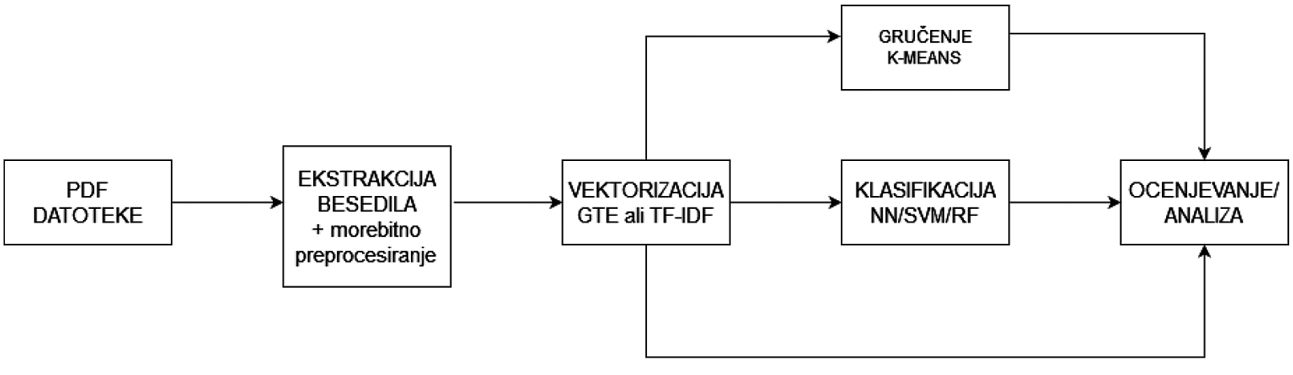
V okviru naše raziskave smo še želeli ugotoviti tudi, ali je trenutna kategorizacija učinkov uporabe odprtih podatkov ustrezna. Naš cilj je bil ugotoviti, ali bi lahko identificirali nove kategorije uporabe odprtih podatkov, kar bi lahko prispevalo k izboljšanju natančnosti, uporabnosti ter razumevanju kategorizacij učinkov. Glede na rezultate pri klasifikaciji smo določili najustreznejšo metodo za vektorizacijo opisov primerov uporabe za nadaljnjo analizo. Na sliki 2 so prikazane faze procesa klasifikacije in analize podatkov, ki smo jih izvajali.

Pri nadaljnji analizi pa smo uporabili metodo K-means - gručenja [36], [37], ki nam omogoča ločevanje na nove kategorije. Ustreznost novih kategorij smo ugotavljali glede na sovpadanje s že obstoječimi kategorijami in pregledom primerov uporabe v posameznih skupinah. Za določanje ustreznega števila skupin (clustrov) smo si pomagali z uporabilo elbow metode [38] in Silhouette analize [39].

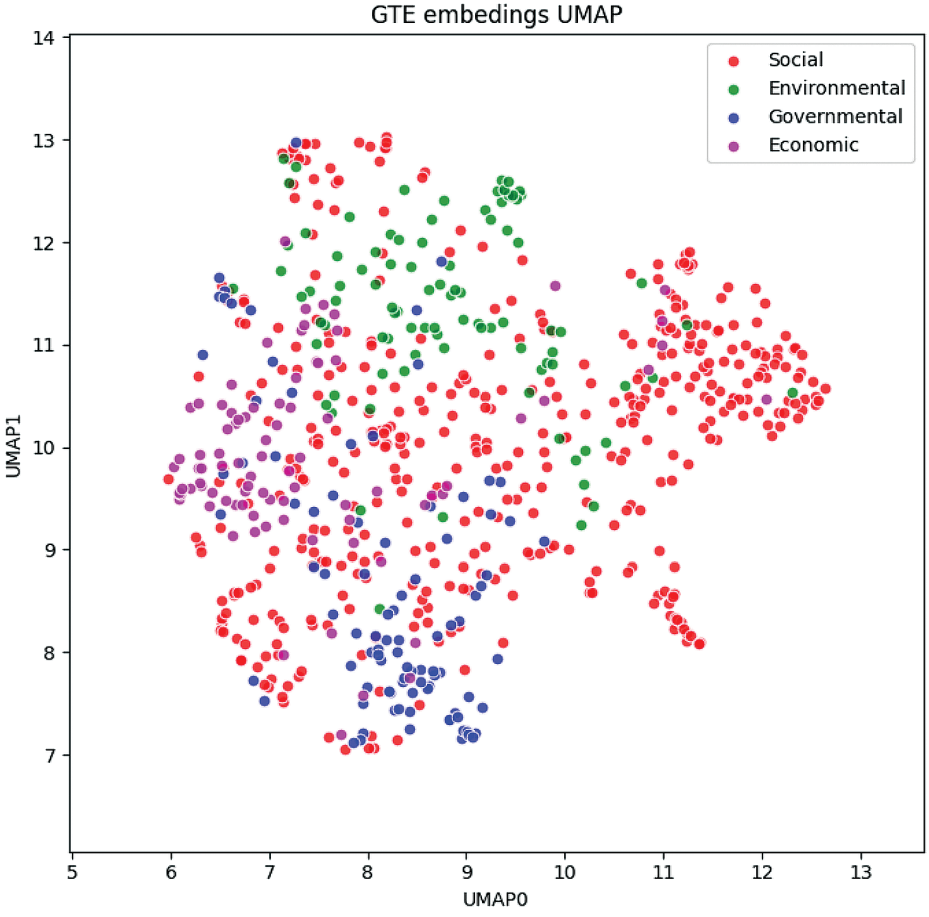
3 REZULTATI

Slika 3 prikazuje UMAP [28] projekcijo vektoriziranih besedil primerov uporabe odprtih podatkov, ki so bili vgrajeni z modelom GTE v1.5 [25], [26] brez preprocesiranja. Besedila so obarvana glede na kategorijo učinka uporabe, ki je bila določena s strani domenskega eksperta. Iz slike je razvidno, da med kategorijami prihaja do prekrivanj, ter da ni jasno razvidnih mej med kategorijami.

Pri klasifikaciji smo najboljše rezultate dosegli z uporabo vektorjev GTE v1.5 [25], [26] modela brez



Slika 2: **Grafični prikaz postopka izvedbe analize.**



Slika 3: **UMAP [28] projekcija vektoriziranih besedil primerov uporabe odprtih podatkov, ki so bili vgrajeni z modelom GTE v1.5 [25] [26] brez preprocesiranja.**

dodatnega preprocesiranja besedila in uporabo nevronske mreže za klasifikacijo teh vektorjev v posamezne kategorije. Rezultati so bili ocenjeni glede na klasifikacijsko točnost (classification accuracy ACC) [40], AUC oceno [41] in F1 oceno [42] (Tabela 3).

Tabela 3: **Primerjava rezultatov uporabe modelov GTE v1.5 [25], [26] ter TF-IDF [19] s preprocesiranjem podatkov in brez preprocesiranja podatkov.**

GTE v1.5.	**Brez preprocesiranja.**			**S preprocesiranjem**		
	ACC	AUC	F1	ACC	AUC	F1
NN	0,80	0,94	0,80	0,72	0,91	0,71
SVN	0,792	0,86	0,79	0,752	0,84	0,76
RF	0,736	0,82	0,74	0,728	0,82	0,72
TF-IDI	**Brez preprocesiranja.**			**S preprocesiranjem**		
	ACC	AUC	F1	ACC	AUC	F1
NN	0,64	0,90	0,63	0,56	0,90	0,55
SVN	0,272	0,51	0,18	0,336	0,57	0,26
RF	0,64	0,80	0,70	0,648	0,75	0,61

Na sliki 4 je prikazana UMAP [28] vizualizacija aktivacij zadnjega skritega sloja klasifikatorja za določanje učinkov uporabe odprtih podatkov glede na opise primerov uporabe. Vizualizacija je razdeljena na dva dela:

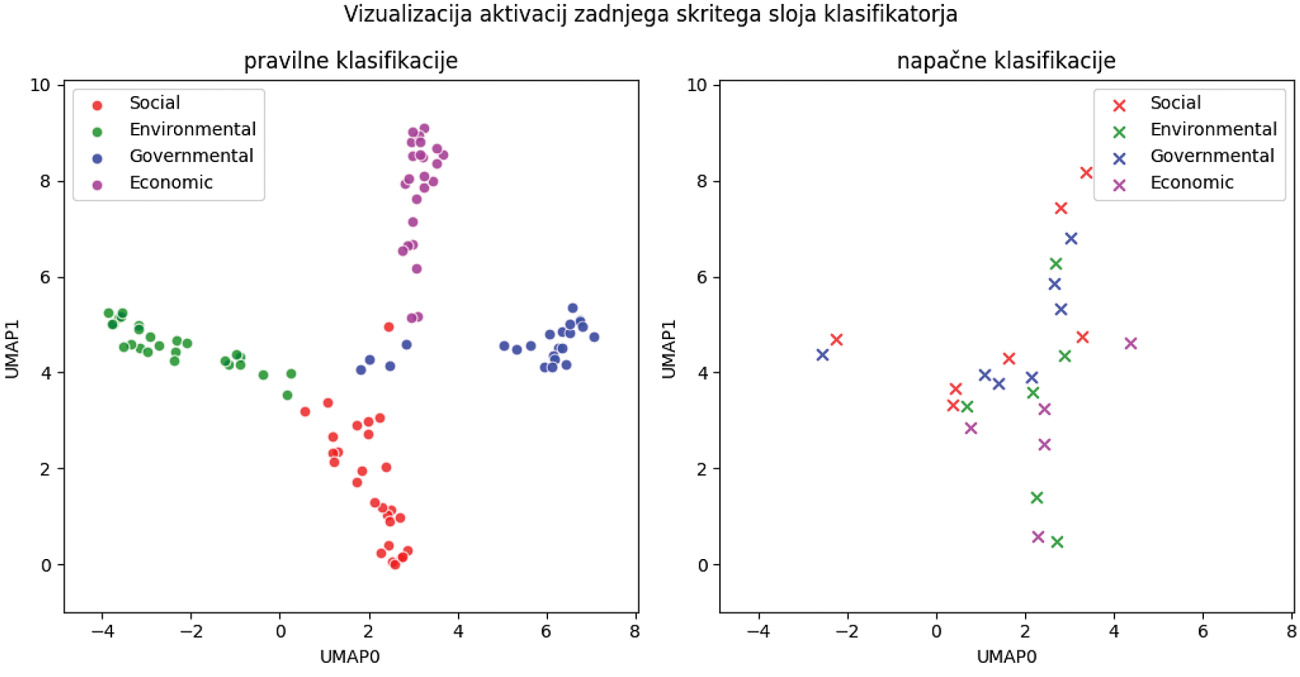
Levi del: Prikazuje aktivacije pravilnih klasifikacij. Pike predstavljajo primere uporabe, ki so bili pravilno razvrščeni v kategorije.

Desni del: Prikazuje aktivacije napačnih klasifikacij. Križci predstavljajo primere uporabe, ki so bili napačno razvrščeni. Barva križca predstavlja pravilno kategorijo.

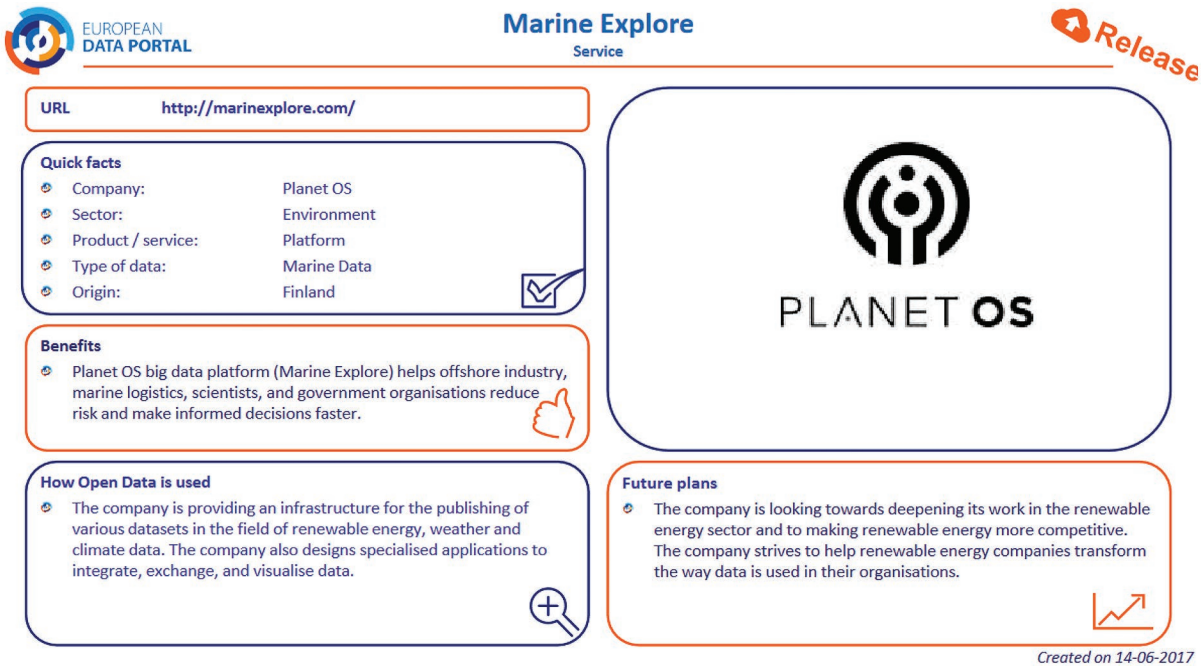
Iz vizualizacije lahko razberemo, da je klasifikator sposoben ločiti med posameznimi kategorijami. Večina napak je pri primerih uporabe, ki so glede na klasifikator povezani z več kategorijami. Napak, kjer predviden vektor spada popolnoma v drugo kategorijo od predvidene s strani domenskega eksperta, ni veliko (dva družbena primera med ekonomskimi (graf zgoraj), dva okoljska in en ekonomski med družbenimi (graf spodaj) in en družbeni in vladni med okolijskimi (graf levo). Te napake bi lahko bile tudi posledica napačnih označb.

Na podlagi te analize lahko sklepamo, da je klasifikator dokaj uspešen pri prepoznavanju kategorij učinkov uporabe odprtih podatkov, vendar obstaja še prostor za izboljšanje, zlasti pri razvrščanju primerov uporabe, ki so povezani z več kategorijami učinka.

Za boljšo predstavitev delovanja klasifikatorja pri primerih učinkov uporabe smo izpisali predvidene verjetnosti kategorij za en primer, kjer se učinek glede na klasifikator kaže v več kategorijah (Slika 5, Tabela 4,5) in primer, pri katerem klasifikator predvideva učinek v eni kategoriji (Slika 6, Tabela 6,7).



Slika 4: **UMAP [28] vizualizacija aktivacij zadnjega skritega sloja klasifikatorja za določanje kategorij učinkov uporabe odprtih podatkov glede na opise primerov uporabe**



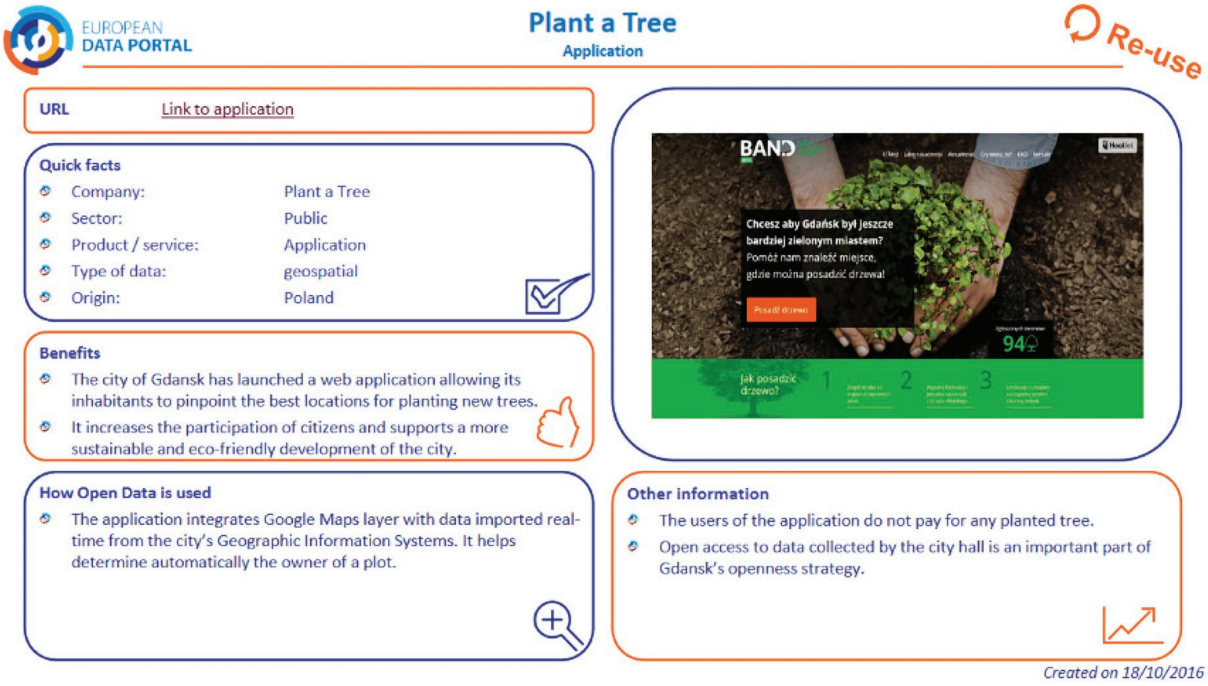
Slika 5: **Zajeta slika PDF dokumenta projekta Marine Explore. [16]**

Tabela 4: **Primer surovega in neprocesiranega besedila projekta Marine Explore, ki smo ga uporabili v analizi.**

Marine Explore \n\nService \n\nURL \n\nhttp://marinexplore.com/ \n\n \n\nQuick facts \n\nCompany: \n\nPlanet OS \n\nSector: \n\n \n\nEnvironment \n\n \n\nProduct / service: \n\nPlatform \n\nType of data: \n\nMarine Data \n\nOrigin: \n\n \n\nFinland \n\nBenefits \n\nPlanet OS big data platform (Marine Explore) helps offshore industry, \n\nmarine logistics, scientists, and government organisations reduce \n\nrisk and make informed decisions faster. \n\nHow Open Data is used \n\nFuture plans \n\nThe company is providing an infrastructure for the publishing of \n\nvarious datasets in the field of renewable energy, weather and \n\nclimate data. The company also designs specialised applications to \n\nintegrate, exchange, and visualise data. \n\nThe company is looking towards deepening its work in the renewable \n\nenergy sector and to making renewable energy more competitive. \n\nThe company strives to help renewable energy companies transform \n\nthe way data is used in their organisations. \n\nCreated on 14-06-2017 Release \n

Tabela 5: **Rezultati predvidenih verjetnosti za razrede oziroma kategorije učinkov OP projekta Marine Explore.**

Primer uporabe	**Resnični razred**	**Predvidene verjetnosti za razrede**			
		EKONOMSKI	OKOLJSKI	VLADNI	DRUŽBENI
Marine Explore	okoljski	0,52	0,23	0,03	0,22



Slika 6: **Zajeta slika PDF dokumenta projektaPlant a Tree. [16]**

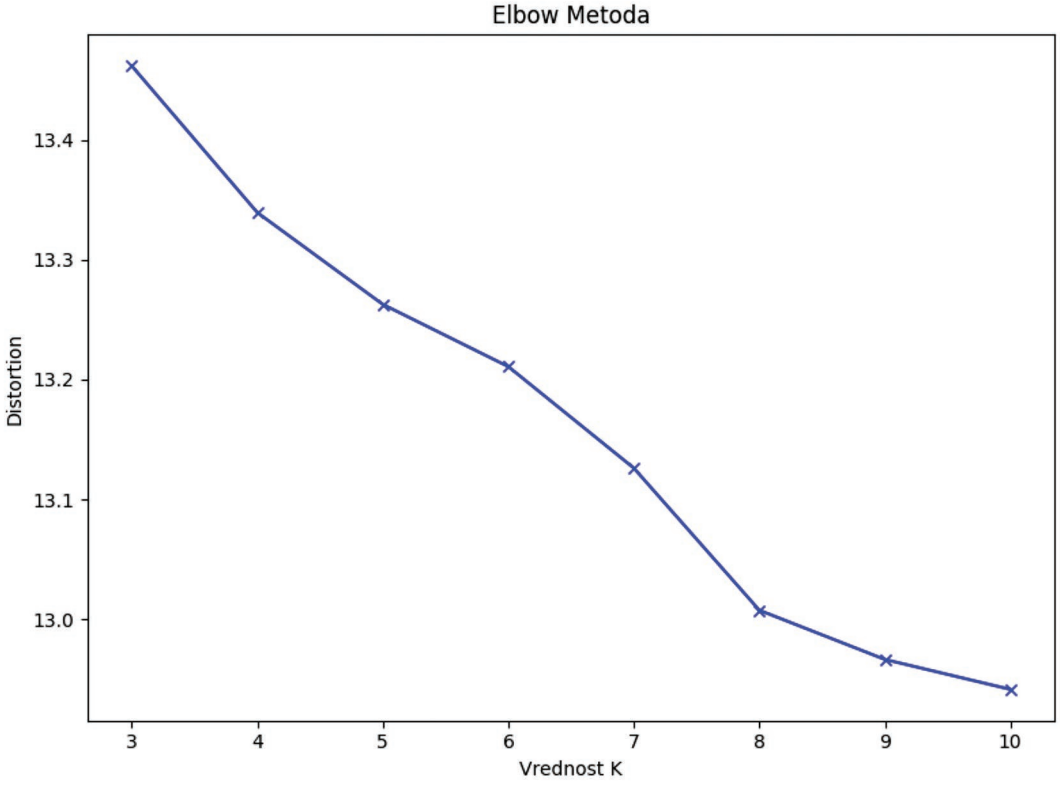
Tabela 6: **Primer surovega in neprocesiranega besedila projekta Plant a Tree, ki smo ga uporabili v analizi.**

Plant a Tree\nApplication\nURL\nLink to application\n\nQuick facts\nCompany:\nPlant a Tree\n\n\nSector:\n\nPublic\n\nProduct / service:\nApplication\nType of data:\ngeospatial\nOrigin:\n\nPoland\nBenefits\nThe city of Gdansk has launched a web application allowing its\ninhabitants to pinpoint the best locations for planting new trees.\nIt increases the participation of citizens and supports a more\nsustainable and eco-friendly development of the city.\nHow Open Data is used\nOther information\nThe users of the application do not pay for any planted tree.\nOpen access to data collected by the city hall is an important part of\nGdansk's openness strategy.\nThe application integrates Google Maps layer with data imported real-\ntime from the city's Geographic Information Systems. It helps\ndetermine automatically the owner of a plot.\n\nCreated on 18/10/2016 Re-use\nCreated on 14-06-2017 Release \n

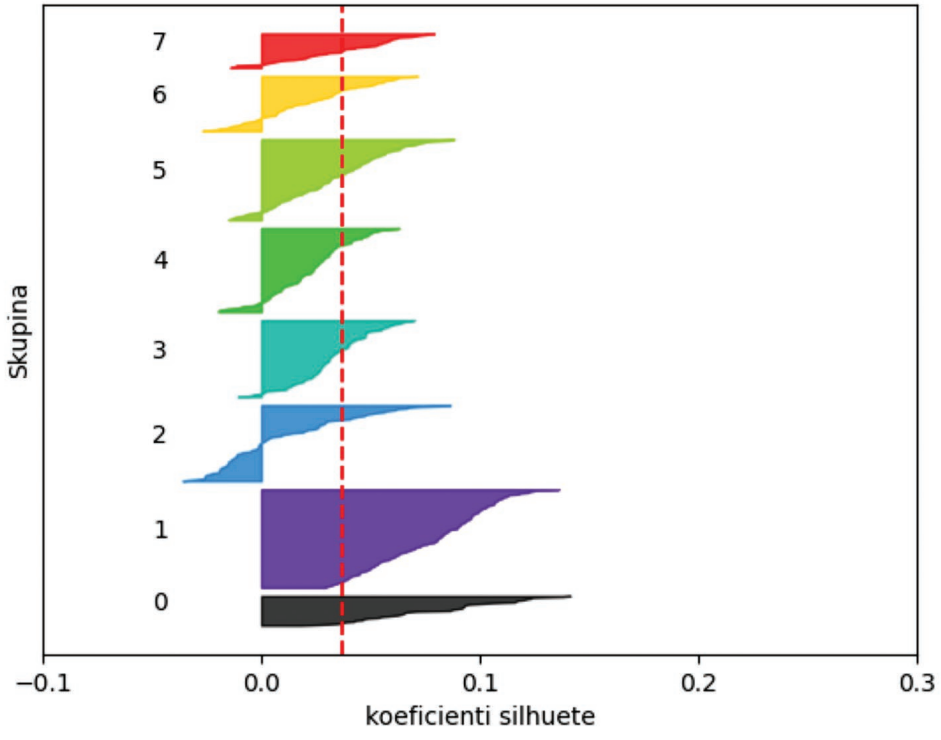
Tabela 7: **Rezultati predvidenih verjetnosti za razrede oziroma kategorije učinkov OP projekta Plant a Tree.**

Primer uporabe	**Resnični razred**	**Predvidene verjetnosti za razrede**			
		EKONOMSKI	OKOLJSKI	VLADNI	DRUŽBENI
Plant a Tree	okoljski	0	0,98	0	0,02

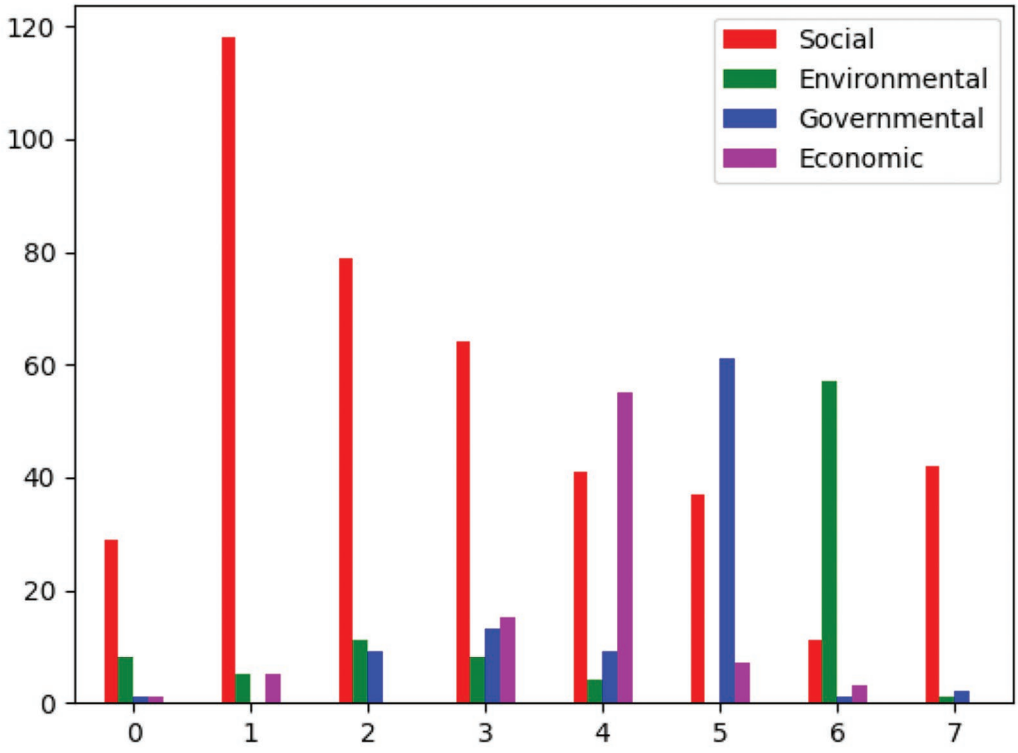
Rezultati, pridobljeni z razvojem klasifikatorja, nakazujejo, da od uporabljenih metod vektorji pridobljeni s pomočjo GTE v1.5 [25], [26] modela brez dodatnega preprocesiranja najbolj natančno zajemajo vsebino opisov uporabe za namen ugotavljanja kategorije učinka. Ker so bili vektorji dovolj deskriptivni za klasifikacijo, smo nadaljevali z analizo teh vektorjev v iskanju morebitnih novih kategorij učinkov, ki bi omogočile bolj natančno in uporabno klasifikacijo učinkov uporabe odprtih podatkov. Z uporabo elbow metode [38] (Slika 7) in Silhouette metode [39] (Slika 8) smo ugotovili, da bi bilo možno učinke razdeliti na 8 skupin z uporabo metode gručenja K-means [36], [37].



Slika 7: **Črtni grafikon distorzije po vrednosti K metode k-means gručenja [36], [37], [38].**



Slika 8: **Vizualizacija koeficientov silhuete [39] za vrednost K=8 za k-means metodo gručenja [36], [37]**



Slika 9: **Stolpčni grafikon prikazuje ujemanje prej določenih kategorij s kategorijami določenimi z k-means metodo gručenja [36], [37] (na x osi so označene k-means kategorije, na y osi pa število primerov uporabe, barve ločujejo prej določene kategorije).**

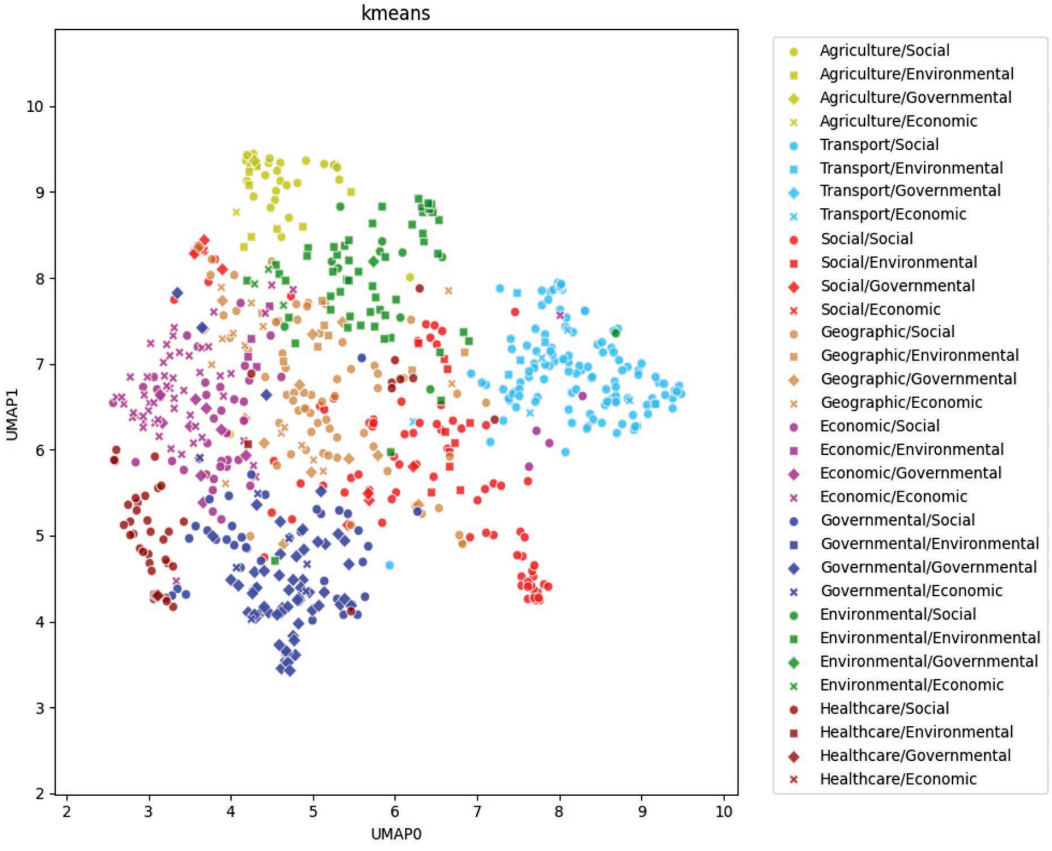
Po uporabi k-means metode gručenja [36], [37] na vektorjih smo novo pridobljene skupine primerjali s prej določenimi kategorijami učinkov uporabe. Opazili smo jasno prekrivanje treh novih skupin s tremi od štirih prej določenih kategorijah učinkov (vladni, okoljski, ekonomski) , kot je razvidno na Sliki 9. V preostale nove skupine so bili večinoma razdeljeni primeri uporabe z učinkom v družbeni kategoriji.

Ob pregledu novih kategorij smo določili nove kategorije učinkov, ki so predstavljene v Tabeli 8.

Slika 10 prikazuje UMAP [28] projekcijo vektoriziranih besedil primerov uporabe odprtih podatkov, ki so bili vgrajeni z modelom GTE v1.5 [25], [26]. Barve ločujejo z kategorije pridobljene z k-means metodo [36], [37]. Oblike oznak pa ločujejo med 4 prej določenimi kategorijami.

Tabela 8: **Predlagane kategorije učinkov.**

K-means skupina	Predlagane kategorije	Ang
0	Kmetijski	Agriculture
1	Transportni	Transport
2	Družbeni	Social
3	Geografski	Geographic
4	Ekonomski	Economic
5	Vladni	Governmental
6	Okoljski	Environmental
7	Zdrvstveni	Healthcare



Slika 10: **UMAP [28] projekcija vektoriziranih besedil primerov uporabe odprtih podatkov, ki so bili vgrajeni z modelom GTE v1.5 [25], [26] z označenimi novimi kategorijami.**

4 ZAKLJUČEK

V tem prispevku smo predstavili način avtomatizacije kategoriziranja učinkov uporabe odprtih podatkov glede na opise primerov uporabe. Pokazali smo, da je z uporabo modelov umetne inteligence možno uspešno kategorizirati primere uporabe v trenutno prepoznane in določene kategorije učinkov s strani Evropske komisije. Pokazali smo, da se učinki posameznih primerov uporabe pogosto kažejo v več kategorijah ter da meje med posameznimi kategorijami niso jasne. Po potrditvi možnosti klasifikacije v trenutno poznane kategorije učinkov z uporabo modelov umetne inteligence smo poskusili identificirati morebitne nove kategorije, ki bi ponudile bolj podroben in uporaben pregled nad kategorijami učinkov uporabe odprtih podatkov. Bolj podrobna klasifikacija kategorij učinkov bi lahko prispevala k kasnejšemu bolj natančnem prepoznavanju učinka, saj bi bilo verjetno potrebno prepoznavati učinek v kategoriji zdravstva drugače kot v kategoriji transporta.

5 LITERATURA

[1] Open Government Data. (b. d.). Organisation for Economic Co-operation and Development. https://www.oecd.org/gov/digital-government/open-government-data.htm. (Dostopano dne: 28. Julij 2024)

[2] Attard, J., Orlandi, F. in Auer, S. (2016). Value Creation on Open Government Data. 2016 *49th Hawaii International Conference on System Sciences (HICSS)*.

[3] Safarov, I., Meijer, A. in Grimmelikhuijsen, S. (2017). Utilization of open government data: A systematic literature review of types, conditions, effects and users. *Information Polity*, 22(1), pp. 1-24.

[4] Ubaldi, B. (2013), Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives. OECD *Working Papers on Public Governance*, No. 22, OECD Publishing, Paris.

[5] Jaeger, P. T. in Bertot, J. C. (2010). Transparency and technological change: Ensuring equal and sustained public access to government information. *Government Information Quarterly*, 27(4), pp. 371–376.

[6] Leviäkangas, P. in Molarius, R. (2020). Open government data policy and value added – Evidence on transport safety agency case. *Technology in Society*, 63(2).

[7] Kalampokis, E., Tambouris, E., in Tarabanis, K. (2013). Linked Open Government Data Analytics. *Electronic Government,* pp. 99–110.

[8] Keserű, J. in James Kin-sing C. (2015). The Social Impact of Open Data. *3rd International Open Data Conference 2015 (IODC).*

[9] Huyer, E. in van Knippenberg, L. (2020). The Economic Impact of Open Data: Opportunities for value creation in Europe, Capgemini Invent. *European, Data Portal*.

[10] OECD. (2018). Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact. *OECD Digital Government Studies*. OECD Publishing, Paris.

[11] Zuiderwijk, A. in Janssen, M. (2014). Open data policies, their implementation and impact: A framework for comparison. *Government Information Quarterly*, 31(1), pp. 17–29.

[12] Ferencek, Aljaž, Kljajić Borštnar, Mirjana, Pretnar Žagar, Ajda. Categorisation of open government data literature. *Business systems research*. 2022, vol. 13, no. 1, str. 66–83

[13] Ferencek, Aljaž, Kljajić Borštnar, Mirjana. Topic modelling of open government data impact areas using GPT 3.5 model. V: Drobne, Samo (ur.), et al. *SOR ,23 : proceedings of the 17th International Symposium on Operational Research in Slovenia : Bled, Slovenia, September 20–22, 2023*. 1st electronic version. Ljubljana: Slovenian Society Informatika – Section for Operational Research, 2023. Str. 71–76

[14] Ferencek, Aljaž, Kljajić Borštnar, Mirjana. Open government data impact areas identification with data mining techniques. V: Drobne, Samo (ur.), et al. *SOR ,21 proceedings : the 16th International Symposium on Operational Research in Slovenia : September 22–24, 2021*, online. Ljubljana: Slovenian Society Informatika, Section for Operational Research, 2021. Str. 101-106.

[15] Ferencek, Aljaž, Kljajić Borštnar, Mirjana, Pretnar Žagar, Ajda. Text mining approach to research gap definition in open government data. V: Čeh Časni, Anita (ur.), Arnerić, Josip (ur.). *Book of abstracts*. 18th International Conference on Operational Research, KOI 2020, Šibenik, Croatia, 23–25 September, 2020. Zagreb: Croatian Operational Research Society: University, Faculty of Economics and Business, 2020. Str. 56.

[16] Data.europa.eu. (b. d.). Publications Office of the European Union. https://data.europa.eu/en/impact-studies/use-cases. (Dostopano dne: 24. Julij 2024)

[17] OECD. (2018). Open Government Data Report: Enhancing Policy Maturity for Sustainable Impact. *OECD Digital Government Studies*, OECD Publishing, Paris.

[18] European Data Portal. (2023). Open Data Maturity Report 2023. *Publications Office of the European Union*. https://data.europa.eu/sites/default/files/odm2023_report.pdf (Dostopano dne: 28. Julij 2024)

[19] Robertson, S. (2004). Understanding inverse document frequency: on theoretical arguments for IDF. *Journal of Documentation*, 60(5), pp. 503-520.

[20] Campos, R., Mangaravite, V., Pasquali, A., Jorge, A., Nunes, C., & Jatowt, A. (2020). YAKE! Keyword extraction from single documents using multiple local features. *Information Sciences*, 509, 257–289. https://doi.org/10.1016/j.ins.2019.09.013

[21] Hevner, A., March, S., Park, J. in Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly*, 28(1), pp. 75-105.

[22] Wirth, R. in Hipp, J. (2000). CRISP-DM: Towards a standard process model for data mining. *Proceedings of the 4th International Conference on the Practical Applications of Knowledge Discovery and Data Mining.*

[23] McCulloch, W. S. in Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *The Bulletin of Mathematical Biophysics*, 5(4), pp. 115–133.

[24] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A. N., Kaiser, Ł., in Polosukhin, I. (2017). Attention Is All You Need. *Advances in Neural Information Processing Systems*, pp. 5999–6009.

[25] Alibaba-NLP/gte-large-en-v1.5 Hugging Face. (b.d.). https://huggingface.co/Alibaba-NLP/gte-large-en-v1.5 (Dostopano dne: 2. Julij 2024)

[26] Li, Z., Zhang, X., Zhang, Y., Long, D., Xie, P., Zhang, M. in Group, A. (2023). Towards General Text Embeddings with Multi-stage Contrastive Learning.

[27] Devlin, J., Chang, M. W., Lee, K. in Toutanova, K. (2018). BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. *NAACL HLT 2019 – 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies – Proceedings of the Conference*, pp. 4171–4186.

[28] McInnes, L., Healy, J. In Melville, J. (2018). UMAP: Uniform Manifold Approximation and Projection for Dimension Reduction.

[29] Gudivada, V., Apon, A. in Ding, J. (2017). Data quality considerations for big data and machine learning: Going beyond data cleaning and transformations. *International Journal on Advances in Software*, 10(1), pp. 1–20.ž

[30] Ho, T. K. (1995). Random decision forests. *Proceedings of the International Conference on Document Analysis and Recognition*, pp. 278–282.

[31] Cortes, C. in Vapnik, V. (1995). Support-vector networks. *Machine Learning*, 20(3), pp. 273–297.

[32] Hendrycks, D. in Gimpel, K. (2016). Gaussian Error Linear Units (GELUs).

[33] Bridle, J. S. (1990). Probabilistic Interpretation of Feedforward Classification Network Outputs, with Relationships to Statistical Pattern Recognition. *Neurocomputing*, pp. 227–236.

[34] Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I. in Salakhutdinov, R. (2014). Dropout: A Simple Way to Prevent Neural Networks from Overfitting. *Journal of Machine Learning Research*, 15(56), pp. 1929–1958.

[35] Loshchilov, I. in Hutter, F. (2016). SGDR: Stochastic Gradient Descent with Warm Restarts. *5th International Conference on Learning Representations, ICLR 2017 - Conference Track Proceedings*.

[36] Lloyd, S. P. (1957). Least squares quantization in PCM. *Technical Report RR-5497*, Bell Lab, September 1957.

[37] MacQueen, J. B. (1967). Some methods for classification and analysis of multivariate observations. In L. M. Le Cam & J. Neyman (Eds.), *Proceedings of the fifth Berkeley symposium on mathematical statistics and probability*, Vol. 1, pp. 281–297.

[38] Robert Tibshirani, Guenther Walther, Trevor Hastie, Estimating the Number of Clusters in a Data Set Via the Gap Statistic, *Journal of the Royal Statistical Society Series B: Statistical Methodology*, 63(2), pp. 411–423.

[39] Rousseeuw, Peter. (1987). Rousseeuw, P.J.: Silhouettes: A Graphical Aid to the Interpretation and Validation of Cluster Analysis. *Journal of Computational and Applied Mathematics*, Vol. 20, pp. 53–65.

[40] Hossin, Mohammad in M.N, Sulaiman. (2015). A Review on Evaluation Metrics for Data Classification Evaluations. *International Journal of Data Mining & Knowledge Management Process*, Vol. 5, pp. 01–11.

[41] Bradley, A.P. (1997). The use of the area under the ROC curve in the evaluation of machine learning algorithms. *Pattern Recognition*, Vol. 30, pp. 1145-1159.ss

[42] Goutte, C. in Gaussier, E. (2005). A Probabilistic Interpretation of Precision, Recall and F-Score, with Implication for Evaluation. *Advances in Information Retrieval, ECIR 2005 Lecture Notes in Computer Science*, Vol. 3408.

▪

Nejc Čelik je asistent za področje Informacijski sistemi na Fakulteti za organizacijske vede na Univerzi v Mariboru. Njegovi raziskovalni interesi so vezani na uporabo umetne inteligence v organizacijah.

▪

Aljaž Ferencek je doktorski študent na Fakulteti za organizacijske vede na Univerzi v Mariboru. Magisterij je pridobil na isti fakulteti. Njegovi raziskovalni interesi vključujejo podatkovno znanost in odprte podatke, o čemer je že objavil raziskave.

Operacijske raziskave kot orodje in podpora za reševanje kompleksnih problemov in optimizacijo procesov - 30 let SDI-SOR

Lidija Zadnik Stirn[1], Samo Drobne[2]
[1] Univerza v Ljubljani, Biotehniška fakulteta, Jamnikarjeva 101, 1000 Ljubljana
[2] Univerza v Ljubljani, Fakulteta za gradbeništvo in geodezijo, Jamova 2, 1000 Ljubljana
lidija.zadnik@bf.uni-lj.si, samo.drobne@fgg.uni-lj.si

Izvleček

V članku predstavljamo razvoj področja operacijskih raziskav (OR) v svetu in Sloveniji (od leta 1964 dalje) s poudarkom na zgodovini slovenske Sekcije za Operacijske Raziskave (SOR, v letih 1992/1993), ki deluje pod okriljem Slovenskega Društva INFORMATIKA (SDI), tj. SDI-SOR. V prispevku opišemo poslanstvo SDI-SOR in njeno delovanje v Sloveniji, predvsem na mednarodni ravni. Sem sodi niz mednarodnih simpozijev OR v Sloveniji, katerih prvi je bil organiziran jeseni 1993, in mednarodno priznane publikacije SDI-SOR. V ta namen smo analizirali zbornike, monografije in posebne številke revij. Članek zaključujemo z vizijo SDI-SOR v prihodnosti.

Ključne besede: dejavnost OR, zgodovina OR, Slovensko društvo Informatika - Sekcija za operacijske raziskave, SDI-SOR, ustanovitev SDI-SOR, dejavnosti SDI-SOR, simpoziji SOR, publikacije SDI-SOR, vizija SDI-SOR

Operations Research as a tool and support for complex problem solving and process optimisation – 30 years of SSI-SOR

Abstract

In the article, we present the development of the Operations Research (OR) field in general and with a special focus on Slovenia. We provide a historical overview of the field of OR globally and in Slovenia, starting in 1964, with special focus on the establishment of the Slovenian Section for Operations Research (SOR), which is active under the umbrella of the Slovenian Society Informatika (SSI), i.e., SSI-SOR, in 1992/1993. We present the mission of SSI-SOR and its activities in Slovenia, especially in the international context. These include the series of international OR symposia in Slovenia, the first of which took place in autumn of 1993, and SSI-SOR's internationally recognized publications. For this purpose, we analysed the proceedings, monographs, and special journal issues, while the article is concluded with SSI-SOR's proposals and vision for the future.

Keywords: Activities of OR, history of OR, Slovenian Society Informatika – Section for Operations Research, SSI-SOR, foundation of SSI-SOR, SSI-SOR activities, SOR symposia, SSI-SOR publications, SSI-SOR vision

1 UVOD

Ključni element (ključna dejavnost) v vsakdanjem življenju posameznikov, podjetij, organizacij in celo držav je sprejemanje odločitev oziroma proces izbire med različnimi možnostmi ali dejanji. Odločitve so težke in kompleksne. Z odločitvami, ki jih sprejemamo zdaj, odločilno vplivamo na prihodnost. Napačna odločitev, ki je lahko posledica negotovosti, pomanjkanja zanesljivih podatkov, nepoznavanja natančnih ciljev, procesov in dejavnikov, ki nastopajo pri odločitvi, lahko prinese velike negativne finančne, okoljske in družbene posledice. Bohanec (2012) ugotavlja, da se moramo problemov pri odločanju zavedati in pri sprejemanju odločitev uporabljati me-

tode in tehnike za podporo odločanju ter modelirati in analizirati odločitve.

Hitre družbene, ekonomske, podnebne, ekološke, tehnološke in druge spremembe zahtevajo nove odločitve, odpirajo nova vprašanja in skrbi glede prihodnosti na vseh področjih življenja, v okolju, gospodarstvu, socialnem življenju in drugod. Srečujemo se z izzivi, ki iščejo ravnotežje med gospodarsko rastjo in okoljsko vzdržnostjo, zagotavljanjem blaginje in družbene enakosti ter priložnostmi in nevarnostmi razvoja umetne inteligence. Te raznolike in medsebojno prepletene razmere in izzivi zahtevajo inovativno paradigmo glede storitev, upravljanja in vodenja ter potrebo po razvoju interdisciplinarnega procesa odločanja za določanje funkcij in zagotavljanje storitev, od katerih je odvisna predvsem trajnostna blaginja ljudi. Paradigma mora upoštevati tudi številne svetovne in lokalne resolucije, akcijske načrte, protokole in smernice o okolju, podnebnih spremembah, energiji in tehnološkem ter socialnem razvoju (Zadnik Stirn in Grošelj, 2019).

V tem kontekstu deluje v svetu z namenom nuditi podporo pri reševanju tovrstnih izzivov skupina raziskovalcev, katerih področje dela opredeljujemo z nazivom »Operacijske Raziskave« (OR). OR so mlada raziskovalna disciplina, opredeljena kot interdisciplinarna in kot taka posega v vse pore življenja.

O metodah, ki jih OR razvijajo in uporabljajo in njihovi uporabi pri reševanju različnih problemov obstoji veliko publikacij (Bronson in Naadimuthu, 1997; Zadnik Stirn, 2001; Pukkala, 2002; Kant in Berry, 2005; Bouyssou et al, 2006; Saaty, 2006; Weintraub et al, 2007; Jones in Tamiz, 2010; Powell in Baker, 2010; Ragsadale, 2010; Joergensen in Fath, 2011; Curwin in Slater, 2013; Ishizaka in Nemery, 2013; Boucherie in van Dijk, 2017). Malo pa je člankov, ki govore o pomenu OR v družbi in okolju, o OR v Sloveniji, o Slovenski Sekciji za Operacijske Raziskave (SOR) in njenem delu v več kot 30 let obstoja SOR. Prav slednji problematiki je v največji meri posvečen ta prispevek.

V drugem poglavju se ukvarjamo z vprašanjem, kaj OR so in na kratko orišemo zgodovino OR. Tretje poglavje se vrne več kot 60 let nazaj, k prvim začetkom OR v Sloveniji. V nadaljevanju opišemo ustanovitev slovenske Sekcije za Operacijske Raziskave (SOR), ki deluje pod okriljem Slovenskega Društva INFORMATIKA (SDI), torej SDI-SOR, in vključitev SDI-SOR v mednarodno okolje. V petem poglavju je predstavljeno delo SDI-SOR, predvsem organizacija številnih mednarodnih konferenc s področja OR. Šesto poglavje podaja pregled publikacij SDI-SOR. Zadnje poglavje pa zaključimo z vizijo OR in zlasti SDI-SOR.

2 OPERACIJSKE RAZISKAVE

2.1 Kaj so operacijske raziskave

Odgovor na zastavljeno vprašanje ni preprost ali enoznačen ali kratek. Z njim so se ukvarjali že številni avtorji (Gal et al., 1991; Winston, 2005; Lukać in Neralić, 2012; Hillier in Lieberman, 2020). Eno izmed definicij OR, kronološki razvoj najpomembnejših metod/modelov OR (med njimi na primer celoštevilsko programiranje, mrežno planiranje in dinamično programiranje, ki so bili razviti leta 1950, simulacije iz leta 1960 in metode večkriterjalnega programiranja iz leta 1980), klasifikacijo modelov OR in področja OR najdemo na https://www.ifors.org/what-is-or/.

Operacijske raziskave (Operations/Operational Research, Management Science, Industrial Engineering, Unternehmensforschung, Business Analytics,…) sodijo na področje informacijsko-upravljavskih znanosti in predstavljajo tipično interdisciplinarno področje delovanja. OR so veja uporabne matematike, ki uporabljajo metode, kot so matematično modeliranje za dosego optimalnih ali kompromisno/zadovoljivo optimalnih rešitev kompleksnih problemov in tako pomagajo upravljavcem doseči zastavljene cilje s podporo znanstvenih metod. Osnovna orodja/metode, ki jih OR uporabljajo, so optimizacija (optimizacija izbrane ciljne funkcije), statistika, verjetnostni račun, teorija iger, teorija grafov, simulacije, poslovna analitika, odločitvena analitika, ekonometrija, linearno in nelinearno programiranje, teorija zalog, stohastični procesi, sistemska analiza, modeli umetne inteligence, strojno učenje in druge.

Najpogostejša definicija OR je, da so OR področje, ki generira matematične modele realnih procesov s ciljem, da se najde optimalna odločitev pri upravljanju s temi procesi. Tako OR kot nepogrešljiv pripomoček upravljanja označujejo sklop metod in pristopov k prepoznavanju, formalizaciji, algoritmizaciji in izvedbi problemov in njihovih rešitev na vseh področjih delovanja. OR obravnavajo probleme predvsem kvantitativno, v zadnjem času pa tudi kvalitativno, in oblikujejo alternativne, zlasti optimalne, rešitve, med katerimi lahko izbirajo odgovorni nosilci odločanja.

V raziskovalno delo na področju OR se vključujejo strokovnjaki s tehniških, ekonomskih, organizacijskih, informacijskih, ekoloških, družboslovnih in drugih ved. Težko je namreč najti stroko, v kateri odločanje ne bi bilo pomembno. Skoraj vsaka disciplina se srečuje z izzivi pri izbiri med različnimi možnostmi in uporablja različne pristope, modele in metode za podporo pri procesu odločanja.

Nekaj primerov odločanja v različnih strokah:

- v upravljanju in poslovanju se odločanje nanaša na procese, strategije, upravljanje, finance in trženje; voditelji in upravljavci sprejemajo odločitve o investicijah, zaposlovanju, proizvodnji in marketinških strategijah;
- v ekonomiji se ukvarjajo z analizo odločitev, ki vključujejo alokacijo omejenih virov za dosego maksimalne koristi, kar vključuje mikroekonomske odločitve podjetij in gospodinjstev ter makroekonomske odločitve vlade;
- v inženirstvu se odločanje uporablja pri načrtovanju, razvoju, proizvodnji in vzdrževanju sistemov in tehnologij; sprejemajo se odločitve o izbiri materialov, oblikovanju, proizvodnji in reševanju tehničnih težav;
- v zdravstvu se srečujejo z odločitvami glede diagnoze, zdravljenja, upravljanja z bolniki in uporabe zdravstvenih virov;
- v pravu se srečujejo z odločitvami glede razlage zakonov, reševanja pravnih sporov, določanja pravnih strategij in svetovanja strankam; odločanje pa temelji na zakonodaji, sodni praksi in pravnih argumentih;
- v informacijski tehniki/tehnologiji (IT) se odločanje nanaša na primere za izbiro tehnoloških rešitev, razvoj programske opreme, upravljanje IT infrastrukture in reševanje varnostnih vprašanj ob uporabi tehnoloških standardov, strokovnega znanja in analitičnih metod;
- v izobraževanju se izbirajo pedagoške metode, učni cilji in ustrezni učni viri;
- v okoljski znanosti se odločanje nanaša na upravljanje naravnih virov, varstvo okolja, načrtovanje trajnostnih razvojnih projektov in sprejemanje političnih odločitev v zvezi z okoljem.

Ti primeri kažejo, da je odločanje ključna dejavnost v številnih strokah, vključno z znanstvenimi, tehnološkimi, družbenimi, ekonomskimi in ekološkimi področji.

Pri sprejemanju odločitev je tako pomembno upoštevati naslednje postopke:

- prepoznavanje problema, odločitev in ciljev;
- zbiranje informacij, ugotavljanje prednosti, slabosti in tveganja, racionalnih in čustvenih vidikov odločevalcev, se zavedati morebitnih pristranosti in omejitev;
- formulacija ustreznega modela (matematičnega);
- reševanje modela, razvoj in uporaba ustreznih metod vključno s programiranjem in analizo informacij;
- izvedba rešitve in ocena rezultatov.

Cilj uporabe modelov pri odločanju je izboljšati razumevanje zapletenih situacij, napovedati izide in izbrati optimalne odločitve na podlagi razpoložljivih informacij. Uporaba matematičnega modeliranja na temelju ogromnega števila podatkov, študija vseh možnih odločitev, upoštevanja tveganja, uporabi programske podpore, in predvsem izbiri ustrezne metode optimizacije, omogočajo odločevalcem podporo, ki jo OR nudijo.

2.2 Kratka zgodovina in razvoj OR

Začetek OR sega v drugo polovico 20. stoletja. Večina virov označuje kot rojstvo OR leto 1943, ko so reševali problem optimiranja transporta ameriške flote v »operaciji« proti Japonski. Od tu izvira tudi ime discipline (OR), ki počasi dobiva drugo obliko (Hillier in Lieberman, 2020). Dejstvo pa seveda je, da številne metode, ki jih danes uporabljamo na področju OR, segajo še mnogo dlje nazaj.

Leta 1939 je Kantorovič v ruščini (Kantorovič, 1939) objavil teorijo in primere uporabe linearnega programiranja. Matematično gledano je predstavil problem maksimizacije linearne funkcije na konveksnem politopu, ki ga je prikazal na problemu reševanja optimalnega razreza materiala in na tako imenovanem transportnem problemu. Ta objava raziskovalcem na zahodu mnogo let ni bila poznana. Le-ti so prišli do formulacije linearnega programiranja na nekoliko drugačen način (Dantzig, 1951, 1963). Njihovi rezultati pa niso bili dostopni Kantoroviču do konca petdesetih let dvajsetega stoletja, ko je Kantorovič objavil knjigo o optimalnem izkoriščanju virov (Kantorovič, 1959). Kantorovič je leta 1975 skupaj s Koopmannsom prejel Nobelovo nagrado za področje ekonomije, in sicer za prispevek k teoriji optimalne alokacije virov. Leta 1939 je Karush uvedel pogoje za reševanje nelinearnega programiranja (Karush,

1939). Tudi njegovi rezultati so postali znani šele kasneje (Kuhn, 1976).

Največji razmah pa so OR dosegle v času 2. svetovne vojne, ko so se raziskovalci s področja optimizacije ukvarjali z razporeditvijo vojnega materiala in ljudi za vojne operacije na najbolj učinkovit način. Tako je veliko raziskovalcev z različnih področij pripomoglo k zmanjšanju števila žrtev na strani zaveznikov in zmagi. Po vojni je postalo jasno, da se metode OR lahko uspešno uporabijo tudi pri reševanju drugih problemov, na primer optimizaciji poslovanja in problemov v tehniki. Med rešitvami problemov s podporo OR omenimo: optimalno vodenje zalog, izbira optimalne investicijske politike, optimiranje transporta, optimalna razporeditev zaposlenih, problem minimalnih odpadkov pri razrezu materiala, problem optimalne bencinske mešanice pri proizvodnji bencina za letala in drugi.

Poleg Kantoroviča in Dantziga, ki ga smatramo za utemeljitelja metode simpleks (metoda za reševanje linearnega programa), moramo omeniti še Charnesa in Cooperja. Charnes je prvi rešil problem degeneracije v metodi simpleks (Charnes, 1952) in je skupaj s Cooperjem in Rhodesom avtor metode »omejevanja« podatkov, DEA (Data Envelopment Analysis) (Charnes et al., 1978).

Pomembno vlogo pri razvoju in uporabi metod OR imajo raziskovalci na Kitajskem, v ZDA in seveda tudi Evropi. Kitajci so po letu 1958 postavili kot ekonomsko prioriteto kmetijsko proizvodnjo in so pozvali raziskovalce s področja OR k sodelovanju. Najpomembnejšo vlogo je pri tem imel Hua Lo-Keng, ki je za reševanje problemov kmetijstva že leta 1960 predlagal linearno programiranje, katerega poznavanje in uporaba se je po njegovi zaslugi uveljavila na Kitajskem (Salaff, 1972; Lukać in Neralić, 2012).

Pomembno vlogo pri razvoju OR imajo nacionalna društva. Leta 1952 je bilo v ZDA ustanovljeno društvo OR Society of America – ORSA, ki je znano predvsem po eni izmed prvih revij na področju OR, Operations Research Journal. Leta 1953 so v ZDA ustanovili inštitut za upravljanje, The Institute of Management Sciences – TIMS. Leta 1995 sta se ORSA in TIMS združila v INFORMS – The Institute For Operations Research and Management Science, https://www.informs.org/. V INFORMS so včlanjeni tudi OR raziskovalci iz Slovenije, nekateri sodelujejo na INFORMS mednarodnih konferencah, ki jih INFORMS organizira dvakrat letno in kot avtorji člankov pri številnih OR revijah, ki jih izdaja INFORMS, na primer OR/MS Today, Mathematics of OR, Management Science, Decision Analysis, INFORMS Journal on Computing, Interfaces in številne druge. Leta 1953 je bilo ustanovljeno društvo OR tudi v Veliki Britaniji (Operational Research Society – ORS). Sledila so številna druga združenja, kot: ALIO (OR društvo držav Latinske in Južne Amerike, http://www.alio-online.org), APORS (OR društvo azijsko-pacifiških držav, www.apors.org) in NORAM (OR društvo Severne Amerike, ZDA in Kanade, https://uia.org/s/or/en/1100037200). Nadalje sta razvoj metod OR, kot tudi njihova vse večja uporaba na skoraj vseh podro-

Slika 1: **Predstavniki držav IFORS, ki so prejele certifikat IFORS (julij 2008, konferenca IFORS v Sandtonu, Južna Afrika; vir: IFORS News, 2008, str. 1).**

čjih, botrovala vse večjemu povezovanju strokovnjakov s področja OR na nacionalnih, kot tudi na svetovni ravni. Tako je bila leta 1959 formalno ustavljena mednarodna zveza IFORS (International Federation of Operational Research Societies). Ustanovni člani IFORS so pod pokroviteljstvom treh držav (ZDA, Velika Britanija, Francija) že leta 1957 v Oxfordu organizirali mednarodno konferenco OR. Za prvo mednarodno konferenco pa IFORS šteje leto 1960. Takrat je IFORS imel že 10 članic (USA, UK, Francija, Australija, Belgija, Kanada. Indija, Nizozemska, Norveška in Švedska) (https://www.ifors.org/history/). Danes ima IFORS 54 članic, to je nacionalnih društev OR (https://www.ifors.org/national-societies/), med njimi je od leta 2007 tudi SDI-SOR. IFORS organizira mednarodne konference iz OR vsako tretje leto. Na konferenci IFORS leta 2008 v Sandtonu (Južna Afrika), ko je IFORS praznoval svojo 50-letnico obstoja, je IFORS podelil svojim aktivnim članicam plakete (slika 1). Prejela jo je tudi SDI-SOR (slika 2). O SDI-SOR je obsežneje napisano v Ittmann (2008). IFORS izdaja tudi številne revije s področja OR: IFORS News, International Transactions in Operational Research, Sustainability Analytics and Modelling (https://www.ifors.org/sustainability-analytics-and-modeling/) in druge https://www.ifors.org/publications/.

Na predlog belgijskega društva OR je bilo leta 1975 s podporo še danskega in nemškega društva OR ustanovljeno evropsko združenje OR pod dežnikom IFORS, in sicer z imenom EURO (Association of European Operational Research Societies, https://archive.ph/20141016111844/http://www.euro-online.org/web/pages/1454/history-of-euro). Istega leta je bila v Brusselsu tudi prva konferenca EURO. EURO izdaja več znanstvenih revij: European Journal of Operational Research (EJOR), EURO Journal on Computational Optimization (EJCO), EURO Journal on Decision Processes (EJDP), EURO Journal on Transportation and Logistics (EJTL) (https://www.euro-online.org/web/pages/106/publications).

3 OPERACIJSKE RAZISKAVE V SLOVENIJI (PRVI ZAČETKI)

OR so se v Sloveniji pojavile v začetku šestdesetih let prejšnjega stoletja, čeprav je bilo nekaj slovenskih strokovnjakov seznanjenih z dognanji na področju OR v svetu že prej. Takrat sta Slovensko društvo ekonomistov in Gospodarska zbornica Slovenije v Ljubljani organizirala simpozij z naslovom »Mehanografija (obdelava podatkov) in OR«, na katerem je bilo 30 predavanj/prispevkov. Simpozij je bil sestavljen iz dveh delov, prvi je obravnaval problematiko pridobivanja in obdelave podatkov, drugi pa OR. V prvem delu so predstavniki različnih podjetij in institucij poročali o povečanju količine informacij, ki zahteva racionalnejši način pridobivanja in obdelave podatkov. Govorniki so poročali o izkušnjah in težavah pri pridobivanju in obdelavi podatkov. Nekateri so predstavili tudi praktične izkušnje in teoretične zasnove. Ta dvojnost je poudarila trdno povezavo med teorijo in prakso. V drugem delu je bila OR predstavljena kot nova znanost za podporo odločanju na številnih področjih. Podanih je bilo več praktičnih primerov iz industrijske proizvodnje, izbire lokacije, prometa, kmetijstva, investicij in zdravstva, kjer sta kot metodi prevladovala linearno programiranje in dvostopenjski proizvodni proces, podprt z linearnim programom. Prispevki so natisnjeni v zborniku konference (Zbornik, 1964). Programski in organizacijski odbor sta vodila profesor V. Rupnik in profesor A. Vadnal. Ta simpozij je pomenil začetek sistematične raziskovalne, pedagoške in svetovalne dejavnosti na področju OR v Sloveniji. Glavni sporočili simpozija

Slika 2: **Lidija Zadnik Stirn, predsednica SDI-SOR, in Elise del Rosario, predsednica IFORS, ki je predala člansko plaketo Sloveniji (julij 2008, konferenca IFORS v Sandtonu, Južna Afrika; vir: IFORS News, 2008, str. 8).**

sta bili: (i) povezava med pridobivanjem/obdelavo podatkov in OR je nujna, saj OR potrebuje trdne numerične podatke o problemu, ki ga je treba rešiti, in (ii) uspešno delo OR je možno le v timskem delu.

Leta 1967 sta Zveza ekonomistov Jugoslavije in Zveza ekonomistov Slovenije na Bledu organizirali konferenco z naslovom »Consultation on the use of OR methods in organizations/institutions in Yugoslavia«, na kateri je bilo predstavljenih 33 prispevkov. Zbornik referatov je bil objavljen kot Zbornik (1967). Problemi, predstavljeni na tej konferenci, so bili s področja proizvodnje, bančništva, prometa, kmetijstva, živilske industrije in turizma. Med metodami je prevladovalo linearno programiranje, zajete pa so bile tudi metode čakalnih vrst, metode mrežnega programiranja, metode razvejanja in dinamičnega programiranja ter nekatere razširitve metode Simplex.

V letu 1974 so se začeli tradicionalni jugoslovanski simpoziji OR, znani pod imenom SYM-OP-IS. Te simpozije so na jugoslovanski ravni organizirali Fakulteta za organizacijske vede, Inštitut za industrijsko ekonomiko in Inštitut Mihajlo Pupin (vsi iz Beograda, Jugoslavija). Simpoziji so potekali vsako leto v Herceg Novem. Udeleževalo se jih je od 150 do 200 udeležencev iz vse Jugoslavije, nekateri tudi iz tujine. Prispevki na simpozijih SYM-OP-IS so bili objavljeni v zbornikih, ki so redno izhajali kot del vsakega simpozija. V zborniku (SYM-OP-IS '86, 1986) so, na primer, objavljeni celotni prispevki 154 predavanj z naslednjih področij: matematično programiranje, kombinatorična optimizacija, mrežno programiranje, grafi, stohastični procesi, večkriterjalne metode, simulacije, napovedovanje, informacijski sistemi, ekspertni sistemi, aplikacije OR s področja proizvodnje, transporta, prometa in poslovne aplikacije. Številni raziskovalci na področju OR iz Slovenije, ki je bila takrat del Jugoslavije, so vsako leto do leta 1990 aktivno sodelovali na SYM-OP-IS-u.

Leta 1974 se je na Ekonomski fakulteti Univerze Edvarda Kardelja v Ljubljani (danes Univerze v Ljubljani) začel izvajati magistrski program Operacijske raziskave, ki se je nekaj let pozneje razširil v doktorski program Informacijske in upravljalne vede. Študenti tega programa so bili diplomanti ekonomije, matematike, fizike, strojništva, elektrotehnike, gradbeništva, prava, sociologije in drugih smeri, ki so po diplomi delali ali še delajo na področju operacijskih raziskav na univerzah, inštitutih in v raziskovalnih oddelkih podjetij.

Istega leta je profesor V. Rupnik izdal knjigo Oris operacijskih raziskav v slovenskem jeziku (Rupnik, 1974). Gre za prvo obsežno knjigo v slovenskem jeziku s področja operacijskih raziskav. Da bi knjiga dosegla širši krog bralcev, ne sledi strogemu vzorcu učbenika, ki običajno predpostavlja določeno znanje matematike in statistike. Bolj gre za pregled problematike, različnih orodij/metod OR pa se dotakne kot drugotnega cilja. Gre torej za sistematično razlago številnih resnih teoretičnih in praktičnih vprašanj, ki zadevajo operacijske raziskave.

4 USTANOVITEV SLOVENSKE SEKCIJE ZA OR IN NJENA VKLJUČITEV V MEDNARODNO OKOLJE

Leta 1991 se je veliko strokovnjakov s področja OR iz Slovenije udeležilo 1. mednarodne konference OR (KOI'91), ki jo je v Zagrebu organiziralo istega leta ustanovljeno Hrvaško društvo OR (HDOI). Po vzoru kolegov s Hrvaške smo strokovnjaki OR Slovenije konec leta 1992 ustanovili svoje združenje, in sicer slovensko Sekcijo za operacijske raziskave (SOR) pod dežnikom Slovenskega društva INFORMATIKA (SDI), torej SDI-SOR, ki danes šteje 107 članov. Za predsednika SDI-SOR je bil izvoljen V. Rupnik (1992-1997), za tajnika pa S. Drobne (1992-).

SDI-SOR je forum za raziskovalce in praktike z vseh področij OR in sorodnih področij, ki sodijo med discipline in programe upravljanja virov in izobraževanja ter uporabljajo orodja, kot so linearno in nelinearno programiranje, diskretna in kombinatorična optimizacija, stohastično odločanje, večkriterijska optimizacija, strateške igre, teorija zalog, teorija grafov, dinamična optimizacija, upravljanje sistemov, teorija kontrole in druga. SDI-SOR je na svoji prvi seji konec leta 1992 začrtala področja delovanja in opredelila cilje sekcije, kot so podpirati in spodbujati raziskave, razvoj, uporabo in izobraževanje na področju OR, ki vključujejo tudi matematiko, ekonomijo, informatiko, računalništvo, statistiko, okoljsko ekonomijo in teorijo sistemov ter več drugih disciplin. Zato je interdisciplinarni in aplikativni znanstveni značaj OR ena od glavnih skrbi SDI-SOR. V glavne dejavnosti, v katere naj bi se usmerili člani SDI-SOR, podpirajo poslanstvo SDI-SOR, tj. povečanje prepoznavnosti in vpliva OR ter tesnejše sodelovanje z izobraževalnimi ustanovami, industrijo, podjetji, vlado in mednarodnimi institucijami, lahko strnemo kot (Zadnik Stirn in Drobne, 2022):

- publiciranje temeljnih in aplikativnih raziskovalnih dosežkov z referati, članki in monografijami; to aktivnost so člani SDI-SOR v veliki meri tekom let (1992-2023) uspešno izvajali na domači in predvsem mednarodni ravni; člani SDI-SOR so napisali vrsto člankov za 17 Zbornikov mednarodnih konferenc OR v Sloveniji, uredili te zbornike, napisali in uredili 4 monografije, bili člani uredniških odborov mednarodnih revij s faktorjem vpliva, recenzenti, napisali številne članke objavljene v domačih in mednarodnih revijah s področja OR, itd. (več o objavah članov SDI-SOR je zapisano v naslednjih poglavjih);
- vključevanje OR v pedagoški proces – tu je SDI-SOR delno uspešna; na Ekonomski fakulteti, Strojni fakulteti, Biotehniški fakulteti, Fakulteti za gradbeništvo in geodezijo, in nekaterih drugih fakultetah UL, na Ekonomsko-poslovni fakulteti in Fakulteti za organizacijske vede, Univerze v Mariboru (UM), in številnih drugih, se izvajajo moduli oziroma predmeti s področja OR, vendar je tu še veliko prostora za intenzivneje izvajanje pedagoškega procesa s področja OR na vseh stopnjah študija. So pa člani SDI-SOR kot gostujoči profesorji ali vabljeni predavatelji delovali tudi na številnih tujih univerzah in inštitutih;
- seznanjanje gospodarskih subjektov in javnosti z možnostjo uporabe OR; tudi na tem področju je bila SDI-SOR doslej še veliko premalo aktivna;
- sodelovanje pri organizaciji domačih in mednarodnih srečanj; to aktivnost so člani SDI-SOR vsa leta intenzivno izvajali z organizacijo mednarodnih simpozijev v Sloveniji, sodelovanju na EURO in IFORS konferencah, sodelovanju na konferencah Hrvaškega, Avstrijskega, Nemškega in drugih društev OR, sodelovanju na konferencah informatike, zlasti DSI, statističnih konferencah, zlasti Hrvaškega statističnega društva, konferencah IFIP TC7, konferencah Večkriterijskega odločanja, ki jih je organizirala Ekonomska fakulteta v Katowicah, Poljska, in številnih drugih;
- vključitev v mednarodna združenja, ki se ukvarjajo z OR, kot so IFORS, EURO; SDI-SOR je je bila sprejeta v IFORS leta 2007 na konferenci IFORS v Sandtonu (Ittmann, 2008), leta 2008 pa je SDI-SOR postala članica EURO; člani SDI-SOR aktivno delujejo v IFORS in EURO in sicer v njihovih odborih, komisijah, na primer, vodili so komisijo za najvišjo nagrado EURO – EURO Distinguished Service Award - EDSA) in sekcijah, pri organizaciji konferenc in predstavitvi referatov na teh konferencah; številni naši člani so imeli na teh konferencah tudi vabljena predavanja.

Več podrobnosti o delu SDI-SOR v letih 1997-2002 je v prispevku Zadnik Stirn (2002). Poročila o delu SDI-SOR za nadaljnja leta pa so kot Poročilo SDI-SOR za leta 2005, …, 2023 na https://www.drustvo-informatika.si/sekcije-drustva/poročilaSOR.

5 ORGANIZACIJA MEDNARODNIH SIMPOZIJEV OR

Med najpomembnejšimi dejavnostmi članov SDI-SOR je organizacija mednarodnih simpozijev OR v Sloveniji, znanih kot SOR'93, SOR'94 ... SOR'21, in jubilejnega simpozija SOR'23, ki je septembra 2023 potekal na Bledu in je bil posvečen 30-letnici SDI-SOR (slika 3). Sprva so bili ti simpoziji organizirani vsako leto, pozneje, od leta 1997 dalje, pa jih SDI-SOR organizira na vsaki dve leti. Člani SDI-SOR so tudi soorganizatorji bienalnih simpozijev iz OR na Hrvaškem. Aktivno sodelujejo tudi na konferencah INFORMS, IFORS, EURO in drugih.

Leta 1993 je SDI-SOR ob podpori Ministrstva za znanost in tehnologijo Republike Slovenije in Ekonomske fakultete Univerze v Ljubljani organizirala 1. simpozij iz OR, SOR'93, na nacionalni ravni. Poročilo SDI-SOR o SOR'93 je na spletni strani https://www.drustvo-informatika.si/sekcije-drustva/SOR/porocilaSOR.

V obdobju 1993–2023 je SDI-SOR organizirala skupno 17 mednarodnih simpozijev s področja OR. Od leta 1994 so ti simpoziji potekali z mednarodno udeležbo, ki se je iz leta v leto povečevala. Kratek pregled glavnih govornikov in sekcij ter držav, iz katerih so prišli glavni govorniki, je v preglednici 1. Simpozije so podprle članice slovenskih univerz, ministrstva Republike Slovenije, tuje institucije, združenja in društva (hrvaško, nemško, avstrijsko, madžarsko, poljsko društvo in druga), EURO, IFORS ter številne druge institucije in posamezniki.

Simpoziji SOR so prvi znanstveni dogodek na področju OR v Sloveniji in predstavljajo mednarodni forum za znanstveno izmenjavo na področjih OR, matematike, statistike, ekonomije, inženirstva, izobraževanja, okolja, informatike, računalništva in drugih področij.

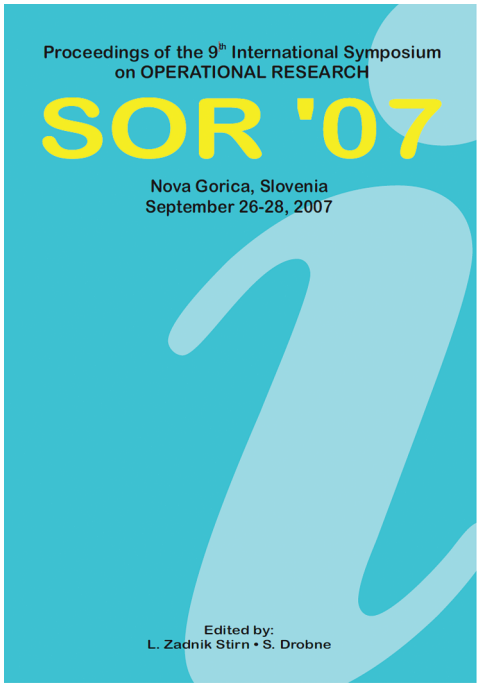
Od leta 1997 organizira SDI-SOR v dogovoru s HDOI simpozij vsaki dve leti, kar pomeni, da SDI-

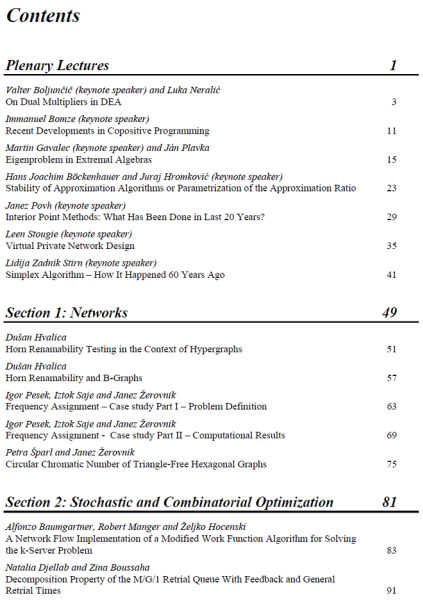
Slika 3: **30 let SDI-SOR (predstavniki EURO in SDI-SOR, 20. september 2023, konferenca SOR'23 na Bledu, Slovenija).**

-SOR in HDOI organizirata mednarodni simpozij OR, in sicer, eno leto v Sloveniji, drugo leto na Hrvaškem. Tako je SDI-SOR organizirala SOR'93, SOR'94, SOR'95, SOR'97, SOR'99, SOR'01, SOR'03, SOR'05, SOR'07, SOR'09, SOR'11, SOR'13, SOR'15, SOR'17, SOR'19, SOR'21 in SOR'23. Prispevki, predstavljeni na teh simpozijih, so bili recenzirani in objavljeni v zbornikih posameznih simpozijev (Proceedings of the ... (2023), (2021), (2019) ... (1993)). Zborniki so na voljo tudi v elektronski obliki na naslovu https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor, do katerega lahko dostopate tudi s spletne strani simpozijev https://sor.fov.um.si/publications/. Podrobna poročila o simpozijih so na voljo na spletni strani https://www.drustvo-informatika.si/sekcije-drustva.

Na simpozijih SOR je bilo predstavljenih 1110 recenziranih prispevkov, ki so bili objavljeni v 17 zbornikih, indeksiranih v Current Mathematical Publications, Mathematical Review, Zentralblatt fuer Mathematik/Mathematics Abstracts, MATH na STN International in CompactMath, INSPEC in drugih. Primer naslovnice in prve strani (vsebina) Zbornika simpozija iz leta 2007, to je SOR'07, je na sliki 4.

Največje število prispevkov, predstavljenih na SOR'21, je bilo 118, najmanjše število prispevkov, predstavljenih na SOR'95, pa je bilo le 21. Povprečno število predstavljenih in v zborniku objavljenih prispevkov je bilo 65,29 prispevka na simpozij. Avtorji iz 26 držav so imeli skupaj 105 plenarnih predavanj. Predstavitve na simpozijih so bile razdeljene na sekcije. Na vseh simpozijih je bilo 157 sekcij, največ na SOR'21, in sicer 19 (11 posebnih sekcij in 8 sekcij z ostalimi prispevki), povprečno pa je bilo 9,06 sekcije na simpozij. V preglednici 1 si lahko ogledamo tudi, katere sekcije so bile najpogostejše, ponavljajoče se in posebej zanimive, in si ustvarimo predstavo o vsebini predstavljenih prispevkov. Prispevke, ki so bili tam predstavljeni in objavljeni, je napisalo 1964 avtorjev. Največje število avtorjev je bilo zabeleženo na SOR'21 (240), najmanjše na SOR'95 (28), povprečno število avtorjev na simpozij pa je bilo 110,51. Avtorji so prihajali z vsega sveta, največ jih je bilo seveda iz Slovenije in sosednjih držav (Hrvaška, Madžarska, Avstrija, Italija, Češka, Slovaška, Nemčija ...).





Contents

Slika 4: **Primer izvoda Proceedings SOR'07 z naslovnico in prvo stranjo vsebine**

Največ držav je bilo predstavljenih na simpoziju SOR'17 (25), najmanj pa na simpoziju SOR'93 (le 1, saj je šlo za nacionalni simpozij), povprečno število držav na simpozij pa je 12,56.

Člani SDI-SOR aktivno sodelujejo na vseh EURO konferencah, kjer organizirajo sekcije, so člani Programskih odborov, vabljeni predavatelji, soizdajatelji zbornikov, nadalje so člani komisij EURO, člani Upravnega odbora EURO in drugo. Nadalje sodelujejo na vseh konferencah IFORS, kjer organizirajo sekcije, so člani Programskih odborov, so člani Upravnega odbora IFORS in dopisni člani IFORS News in drugo. Sodelujejo tudi s Češkim društvom OR; na primer, v leta 1998 so z vabljenim predavanjem aktivno sodelovali na 11th Joint Czech-German-Slovak Conference: Mathematical Methods in Economy and Industry v Liberecu. Leta 1998 je SDI-SOR soorganizirala Austrian-Croatian-Slovenian Workshop in OR v Seggaubergu, Austria, kjer je bila gostiteljica Univerza v Grazu. Nenazadnje pa člani SDI-SOR aktivno sodelujejo z vabljenimi predavanji, referati, kot recenzenti, člani Programskega odbora in vodje sekcij na vseh mednarodnih konferencah, ki jih organizira HDOI, Hrvaška, to je na International Conference on Operational Research KOI'xx, kjer se xx nanaša na KOI'1992, …, KOI'2022. Sodelujejo tudi v IFIP, katerega član je SDI, in sicer na IFIP TC7 konferencah z referati, kot člani Programskih odborov in so člani Upravnega odbora. Sodelovali so z referati, kot recenzenti, člani Programskega odbora in vodje sekcij na Dnevih slovenske INFORMATIKE (DSI), v zadnjih letih žal v manjšem obsegu.

6 PREGLED PUBLIKACIJ SDI-SOR

6.1 Monografije

Večina članov SDI-SOR je povezana z univerzami ali inštituti. Zato so člani večinoma raziskovalci s področja operacijskih raziskav in sorodnih področij. Nekateri od njih so skupaj s kolegi iz tujine, večinoma iz Hrvaške, svoja dela zbrali v obliki monografij. Od leta 1998 je SDI-SOR izdala pet monografij: Rupnik (1998), Rupnik et al. (2000), Zadnik Stirn et al. (2005), Rupnik in Sundać (2005) ter Rupnik (2013).

Monografija (Rupnik, 1998) je razdeljena na šest poglavij, ki sledijo uvodu in se končajo s citirano literaturo. V prvem poglavju so predstavljene osnove teorije ekonomske integriranosti, v drugem in tretjem poglavju pa sta diagnosticirani horizontalna in vertikalna ekonomska integriranost. Četrto in peto poglavje predstavljata napovedovanje horizontalne in vertikalne ekonomske integrabilnosti. V zadnjem (šestem) poglavju avtor ugotavlja uporabnost metodologije integracije v preteklosti in prihodnosti.

Preglednica 1: **Pregled znanstvenih člankov v zbornikih SOR v obdobju 1993-2023 (številka v oklepaju pomeni število prispevkov).**

Zbornik	Plenarni predavatelji	Posebne sekcije	Sekcije
SOR'23 (96)	1. Sevaux EURO/(FR) 2. Sethi (USA) 3. Magron (FR) 4. Pejić Bach (CRO) 5. Kastrin (SI)	1. Applications of OR in Agricultural Economics (8) 2. Applications of OR in Industry and Mechanical Engineering (4) 3. Artificial Intelligence in Business: Obstacles and Perspectives (4) 4. Discrete Optimization Methods and Models for Real-world Problem Domain (15) 5. Industry & Society 5.0: Optimization and Learning in Human and Industrial Environments (9) 6. Game Theory (5) 7. Social Innovations in Ageing Studies Supported by OR Models (7) 8. Unravelling the Business Models of Sharing Economy by Applying Methods of OR and Statistics (3)	1. Econometric Models and Statistics (4) 2. Human Resources (5) 3. Finance and Investments (8) 4. Location and Transport, Graphs and their Applications (7) 5. Mathematical Programming and Optimization (5) 6. Multi-Criteria Decision-Making (7)
SOR'21 (118)	1. Ban (A) 2. Kojić (CRO) 3. Patrinos (B) 4. Sethi (USA) 5. Gros (SI)	1. Application of OR in Smart Cities (6) 2. Computational Mathematical Optimization (13) 3. Data Science - Methodologies and Case Studies (10) 4. Graph Theory and Algorithms (2) 5. High-Performance Computing and Big Data (3) 6. Industry & Society 5.0: Optimization in Industrial and Human Environment 6) 7. International Projects in OR (2) 8. Lessons Learned from the COVID-19 Pandemic (8) 9. Logistics and Sustainability (9) 10. OR in Ageing Studies and Social Innovations (5), 11. OR in Agricultural Economics and Farm Management (5)	1. Econometric Models and Statistics (6) 2. Environment and Social Issues (5) 3. Finance and Investments (6) 4. Location and Transport, Graphs and their Applications (5) 5. Mathematical Programming and Optimization (6) 6. Multi-Criteria Decision-Making (10) 7. Theory of Games (3) 8. Problems Approaching OR (3)
SOR'19 (106)	Bratko (SI) Čižmešija (CRO) Illes (HU) Jozefowska EURO/(PL) Praprotnik (SI)	1. Application of OR in Agriculture and Agribusiness Management (5) 2. Formal and Behavioral Issues in MCDM (7) 3. Graph Theory, Algorithms (12) 4. High-Performance Computing and Big Data (4) 5. Optimization in Human Environments (7) 6. System Modelling & Soft OR (5) 7. Towards Industry 4.0 (5)	1. Econometric Models and Statistics (10) 2. Environment and Social Issues (6) 3. Finance and Investments (11) 4. Location and Transport, Graphs (4) 5. Mathematical Programming and Optimization (9) 6. Multi-Criteria Decision-Making (6) 7. Human Resources (4) 8. Production and Management (6)

Zbornik	Plenarni predavatelji	Posebne sekcije	Sekcije
SOR'17 (93)	1. Bogaerts PRACE/(BE) 2. Leopold-Wildburger (AU) 3. Perc (SI) 4. van Wassenhove (FR) 5. Zekić-Sušac (CRO)	1. Advances in Modelling and Statistical Research of the Western Balkan Countries in the Times of Economic Crisis (8) 2. High-Performance Computing and Big Data and General OR Topics (8) 3. Logistics (5) 4. MCDM – Software and Applications (6) 5. Metaheuristic Optimization (5) 6. Industrial Engineering and Services (5) 7. MRP and Related Systems Approach to Systems Optimization and Control with 7. Applications (5)	1. Econometric Models and Statistics (10) 2. Environment and Human Resources (6) 3. Finance and Investments (5) 4. Location and Transport, Graphs, and their applications (6) 5. Machine Learning (4) 6. Mathematical Programming and Optimization (8) 7. Multiple Criteria Decision Making (4) 8. OR Perspectives: Where we have been, where we can go (3)
SOR'15 (93)	1. Ben Tal (IL) 2. Cabello (SI) 3. Cozzini (IT) 4. Gvozdenović (RS) 5. Weber, Savku, Pinheiro, Azevedo (TR) 6. Wei, Tang (SE)	1. Qualitative Multiple Criteria Decision Making (6) 2. Inventory Research (7) 3. Metaheuristic Optimization (7) 4. Big Data (4)	1. Mathematical Programming and Optimization (7) 2. Graphs and their Applications (5) 3. Multiple Criteria Decision Making (5) 4. Econometric Models and Statistics (10) 5. Production (7) 6. Finance and Investments (7) 7. Location and Transport (7) 8. Environment and Human Resources (9) 9. OR Perspectives (6)
SOR'13 (61)	1. Jukić (CRO) 2. Klavžar (SI) 3. Petitjean (FR) 4. Sotitrov (NLI)		1. Mathematical Programming and Optimization (14) 2. Graphs and their Applications (10) 3. Econometric Models and Statistics (5) 4. Finance and Investments (6) 5. Location and Transport (6) 6. Multiple Criteria Decision Making (8) 7. Production and Inventory (3) 8. Creative core FIS - Simulations (5)
SOR'11 (53)	1. Anderson (DK) 2. Gerhardt, Hamacher, Ruzika (DE) 3. Gurtjahr (AU) 4. Koster (DE) 5. Lukač (HR) 6. Pferschy (AU)		1. Graphs and their Applications (3) 2. Production and Inventory (12) 3. OR Applications in Telecommunication and Navigation Systems (3) 4. Finance and Investments (6) 5. Multiple Criteria Decision Making (6) 6. Pascal2 session (3) 7. Mathematical Programming and Optimization (3) 8. Econometric Models and Statistics (6) 9. Location and Transport (5)
SOR'09 (61)	1. Babić (CRO) 2. Csendes (HU) 3. Grubbstroem (SE) 4. Sniedovich (AU) 5. Trzaskalik (PL) 6. Yuan (SE)		1. Discrete Mathematics and Optimization (9) 2. Multicriteria Decision Making (6) 3. Scheduling and Control (5) 4. Finance and Investments (5) 5. Production and Inventory (5) 6. Location and Transport (6) 7. Environment and Human Resources (6) 8. OR Perspectives (2) 9. Statistics (10)

Zbornik	Plenarni predavatelji	Posebne sekcije	Sekcije
SOR'07 (68)	1. Boljunčić, Neralić (CRO) 2. Bomze (AT) 3. Gavalec, Plavka (CZ), (SK) 4. Boeckenhauer, Hromkovič (CH) 5. Povh (SI) 6. Stougie (NL) 7. Zadnik Stirn (SI)		1. Networks (5) 2. Stochastic and Combinatorial Optimization (5) 3. Algorithms (3) 4. Multicriteria Decision Making (4) 5. Scheduling and Control (4) 6. Location Theory and Transport (4) 7. Environment and Human Resource Management (5) 8. Duration Models (5) 9. Finance and Investment (7) 10. Production and Inventory (7) 11. Education and Statistics (5) 12. OR Communications (7)
SOR'05 (63)	1. Boehm (AT) 2. Manger (CRO) 3. Rupnik (SI) 4. Rupnik, Sundać (SI), (CRO) 5. Castelli, Pesenti, Ukovich (IT)		1. Scheduling and Control (4) 2. Stochastic and Combinatorial Optimization (4) 3. Algorithms (7) 4. Environment and Human Resources (7) 5. Location Theory and Transport (10) 6. Finance and Investment (8) 7. Multicriteria Decision Making (5) 8. Networks (4) 9. Production and Inventory (5) 10.Education and Statistics (3)
SOR'03 (49)	1. Cechlarova (SK) 2. Koechel (DE) 3. Luptačik (AT) 4. Šimundić (CRO) 5. Zlobec (I&S), Compton, Vuong (CA)		1. Algorithms (6) 2. Location Theory and Transport (6) 3. Finance (4) 4. Environment and Human Resources (4) 5. Production and Inventory (8) 6. Scheduling and Control (7) 7. Multicriteria Decision Making (3) 8. Education and Statistics (4) 9. Open OR Problems (2)
SOR'01 (59)	1. Rendl (AT) 2. Šorić (CRO) 3. Schaerf, Di Gaspero (IT) 4. Shawe-Taylor (GB) 5. Ferrari, Manzini, Regattieri, Persona (IT)		1. Algorithms (11) 2. Optimization ((5) 3. Scheduling and Control (4) 4. Networks (4) 5. Production (7) 6. Finance (6) 7. Environment and Human Resources (6) 8. Dynamic Systems (3) 9. Education and Statistics (4) 10. Current Projects in Slovenia and Croatia (4)
SOR'99 (43)	1. Burkard, Fortuna (AT) 2. Mitra, Koutsoukis (GB) 3. Neralić (CRO) 4. Schields (US) 5. Zimmermann (CZ)		1. Optimization and Control (4) 2. Hot Lines Panel Section (4) 3. OR Applications (9) 4. Modelling (9) 5. Production and Inventory (6) 6. Network Analysis (6)

Zbornik	Plenarni predavatelji	Posebne sekcije	Sekcije
SOR'97 (58)	1. Becker, Keuhrer, Leopold-Wildburger (DE), (AT) 2. Grubbstroem (SE) 3. Zimmermann (CZ)		1. Wood Processing and Agriculture (10) Optimization (9) 2. Economic (Systems) Modelling and Control (7) 3. Production (6) 4. Business (System) Modelling and Control (6) 5. Traffic and Transportation (4) 6. OR in Transitional Economies (4) 7. OR Experiences and Practical Solutions (4) 8. Inventory (3) 9. Last Minute Section (2)
SOR'95 (21)	Hill (GB)		Uniform session (20)
SOR'94 (31)	1. Csebfalvi (A&G) (HU) 2. Komlosi (HU) 3. Marinović (CRO) 4. Neralić (CRO) 5. Sethi, Taskar, Zhang (CA) 6. Varga (HU)		1. Production (9) 2. Transport (2) 3. Mathematical Programming (6) 4. Various OR Applications (5) 5. Computer Programs (4)
SOR'93 (37)	1. Barle, Grad (SI) 2. Rupnik (SI)		1. Production (10) 2. Transport (5) 3. Mathematical Programming (4) 4. Multicriteria Decision Making and Environment (6) 5. Various OR Applications (7) 6. Computer Programs (3)

Monografija Rešitve proizvodnih problemov (Rupnik et al., 2000) je sestavljena iz skupno 27 poglavij, razdeljenih v pet delov. V njej 33 avtorjev iz Slovenije in Hrvaške obravnava proizvodni proces z uporabo simulacij v proizvodnji, kombinatorične optimizacije proizvodnje, tehničnega načrtovanja proizvodnje, ekonomskega načrtovanja proizvodnje in tehnično-ekonomskega načrtovanja proizvodnje.

Monografija Izbrani modeli za podporo odločanju za probleme proizvodnje in javne politike (Zadnik Stirn et al., 2005) vsebuje 8 poglavij, ki jih je napisalo 12 avtorjev iz Slovenije in Hrvaške (platnici na sliki 5). V njej sta predstavljeni tako teorija kot tudi uporaba modelov, ki temeljijo na novih metodah OR, za reševanje problemov v proizvodnji in upravljanju (predvsem v javni upravi). Poglavja so naslednja: ekonomsko modeliranje in analiza/merjenje kakovosti, večkriterijska orodja za vrednotenje socialno-ekonomskih in okoljskih programov, meje skupnih funkcij na poliedrih - nov pristop h globalni optimizaciji, proces načrtovanja s stohastičnim povpraševanjem, optimizacija procesa razreza materiala, optimizacija razporejanja v proizvodnem procesu, analiza vpliva razvoja cestnega omrežja na vožnjo na delo (primer Slovenije) in analiza učinkovitosti državne uprave. Monografijo sta recenzirala L. Neralić in S. Indihar. Uvod v monografijo sta napisali L. Zadnik Stirn in L. Ferbar.

Avtorja Rupnik in Sundać (2005) v svoji monografiji navajata, da sta neoliberalna in monetaristična doktrina odprli pot neomejenemu razvoju globalizacije. Ta je imela številne pozitivne in negativne učinke. Družba je pozitivne učinke zlahka sprejela, vendar se sprašuje, ali naj sprejme tudi negativne učinke, ki vodijo v brezposelnost, degradacijo okolja, ekonomsko negotovost, razslojenost družbe ter celo bolezni in smrt. Avtorji modelirajo sistem svetovne globalizacije z modelom, ki temelji na meta-matematiki in simulacijah. Z modelom avtorja ugotavljata, da lahko nekorigirana neoliberalna globalizacija, ki

jo podpira doktrina monetarizma, privede do močne diferenciacije človeštva. Na podlagi modela avtorja podata tudi predloge za ohranitev pozitivnih učinkov globalizacije in odpravo ali vsaj delno rehabilitacijo negativnih.

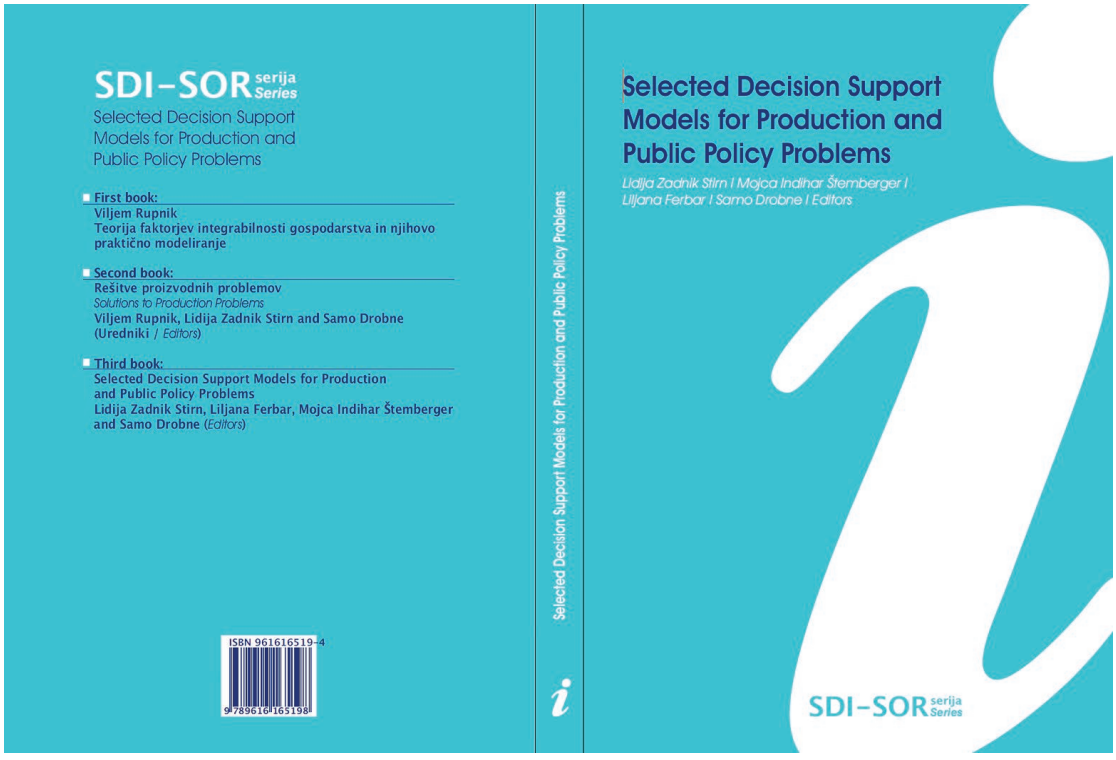
Monografija (Rupnik, 2013) je namenjena ekonomistom, družboslovcem in številnim drugim, ki želijo razmišljati o aktualnih družbenoekonomskih pojavih. Avtor se zaveda, da ima kapital v razvoju pomembno vlogo pri doseganju soglasja o ključnih razvojnih vprašanjih, in se zavzema za trajnostni razvoj. Predlaga »etično« ekonomijo, ki vključuje t. i. informacijsko družbo kot pomembno razsežnost družbe. Poleg empiričnih pristopov njegove ugotovitve in priporočila temeljijo tudi na večparametričnih matematičnih modelih. Predgovoru sledi 17 poglavij, ki obravnavajo neoliberalno globalizacijo (konflikti, posledice in možni popravki), eksistenčni trikotnik družbe, ki ga sestavljajo kapital, narava in delo, ter analizo medsebojnega delovanja med njimi. V zaključkih predlaga etično ekonomijo kot »zdravilo«. Predgovor k monografiji je napisal M. Krisper.

Kot je razvidno iz referenc, so nekatere monografije ali njihovi deli v slovenščini. Dodajmo, da so za slovenski strokovni jezik, tj. slovensko terminologijo na področju OR, publikacije v slovenskem jeziku nepogrešljive in zelo pomembne.

6.2 Člani SDI-SOR aktivno objavljajo in urejajo mednarodne revije s področja OR

Leta 1994 se je SDI-SOR pridružila avstrijskemu, češkemu, hrvaškemu, madžarskemu in slovaškemu društvu za operacijske raziskave pri izdajanju nove revije. Pod vodstvom avstrijskih kolegov je začela izhajati revija Central European Journal for Operations Research and Economic, ki je izhajala do konca leta 1998. Od leta 1999 je revija izhajala pri založbi Physica, pozneje pa pri založbi Springer Verlag pod sedanjim imenom Central European Journal of Operations Research (CJOR). Revija je bila leta 2007 indeksirana v Web of Science. Trenutno je na meji med prvo in drugo polovico revij po faktorju vpliva v kategoriji Web of Science Operations Research and Management Science (Jablonsky et al., 2022).

Člani SDI-SOR so od leta 1997 souredniki revije CJOR. Leta 2011 je SDI-SOR izdala prvo posebno številko z gostujočimi uredniki. Nadalje posebne številke so člani SDI-SOR izdali v letih 2013, 2015, 2017, 2019, 2021 in 2023. Bibliometrična analiza prispevkov, objavljenih v prvih šestih posebnih števil-



Slika 5: **Platnici tretje monografije SDI-SOR**

kah CJOR SDI-SOR, je predstavljena v Kastrin et al. (2021). V tem članku avtorji analizirajo in virtualizirajo letno dinamiko števila objavljenih člankov, izpostavijo najbolj plodne avtorje in države, predstavijo članke z največjim vplivom glede na število citatov ter preučijo mrežo ujemanja ključnih besed, razdeljeno na osem grozdov. Rezultati osnovne analize temeljijo na celotnem naboru 67 člankov iz šestih posebnih številk SDI-SOR, medtem ko razširjena analiza vključuje le 63 člankov iz zbirke WoS in Dimensions.ai. Glede na vrsto objave so vsi članki obravnavani kot izvirni znanstveni prispevki.

Najnovejša številka CJOR (letnik 32, september 2023, številka 3) je ponovno posebna številka SDI-SOR in vsebuje 16 člankov, ki so podrobneje predstavljeni v Povh et al. (2023).

Število člankov v vseh sedmih posebnih številkah CJOR, ki so jih uredili uredniki SDI-SOR, ter imena avtorjev so v Preglednici 2. Iz preglednice je razvidno, da se število člankov, objavljenih v posebnih številkah CJOR SDI-SOR, povečuje. To je posledica večje prepoznavnosti dela SDI-SOR v Srednji Evropi in vse večjega pomena revije CJOR (višji faktor vpliva), kar pomeni, da je zanimanje za objavljanje v tej reviji večje.

Leta 2012 so uredniki revije Business Systems Research (BSR) povabili SDI-SOR k objavi posebne številke (SI). BSR je akademska revija, ki se osredotoča na rezultate raziskav na področju ekonomije in poslovnih sistemov. Poleg tega BSR obravnava tudi raziskave, ki združujejo ekonomijo z drugimi znanstvenimi področji, kot so informacijski sistemi, matematika in družboslovje. BSR preučuje različne poslovne odločitve, procese in dejavnosti v kontekstu dejanskega poslovnega okolja ter v okviru sistemskega pristopa. Revija je indeksirana v Scopusu, Web of Science (ESCI-WoS) in Portalu hrvaških znanstvenih in strokovnih revij. Trenutno je v Scopusu indeksirana kot Q3 za področje ekonomije, ekonometrije in financ. SDI-SOR je od leta 2012 objavila šest posebnih številk: 2012, 2014, 2016, 2018, 2020 in 2022. Posebne številke revije BSR-SI so se osredotočale na nedavne dosežke na področju operacijskih raziskav in znanosti o upravljanju (OR/MS), s posebnim poudarkom na povezovanju OR/MS z drugimi področji kvantitativnih in kvalitativnih metod v multidisciplinarnem okviru (Drobne et al., 2022).

BSR-SI, letnik 13, številka 3, leto 2022, vsebuje deset člankov, ki predstavljajo napredek in nove tehnike (metode) na področju operacijskih raziskav (OR) ter

Preglednica 2: **Število člankov in imena avtorjev v posebnih številkah revije CJOR, ki jih je uredila SDI-SOR v obdobju 2011-2023**.

Leto	Število člankov	Avtorji
2011	8	Bogataj et al., 2011; Grošelj et al., 2011; Hentsch in Köchel, 2011; Ivanov et al., 2011; Jurun in Pivac, 2011; Kovačič in Bogataj, 2011; Matis in Kohani, 2011; Žerovnik in Žerovnik 2011
2013	7	Dumičić et al., 2013; Govorčin et al., 2013; Hvalica, 2013; Kovačič in Bogataj, 2013; Kramberger et al., 2013; Toth in Kresz, 2013; Mladenović et al., 2013
2015	12	Agrež in Damij, 2015; Cechlárová et al., 2015; Dumičić et al., 2015; Gaspars-Wieloch, 2015; Janáček, 2015; Kovačić et al., 2015; Dalpasso in Lancia, 2015; Moeini et al., 2015; Shao in Vesel, 2015; Hunjet et al., 2015; Nguyen in Chassein, 2015; Rudec in Manger 2015
2017	11	Bala et al., 2017; Režnar et al., 2017; Gaspars-Wieloch, 2017; Nikolakopoulos in Ganas, 2017; Bohanec et al., 2017; Mihelčić in Bohanec, 2017; Jánošíková et al., 2017; Janáček in Kvet, 2017; Chocholatá in Furková, 2017; Shao et al., 2017; Hladik, 2017
2019	14	Garajová et al., 2019; Tavakoli in Klavžar, 2019; Trzaskalik et al., 2019; Kadoić et al., 2019; Ligardo-Herrera et al., 2019; Sternad Zabukovšek et al., 2019; Jánošíková et al., 2019; Brelih et al., 2019; Pavlovčič Prešeren et al., 2019; Jordan et al., 2019; Furková, 2019; Jakšić et al., 2019; Čampelj et al., 2019; Bokal in Steibacher 2019
2021	15	Hladík, 2021; Tomanová in Holý, 2021; Jakšić et al., 2021; Cechlárová et al., 2021; Trzaskalik, 2021; Jukić in Sabo, 2021; Matejaš et al., 2021; Janáček in Kvet, 2021; Vrankić et al., 2021; Drnovšek et al., 2021; Furková in Chocholatá, 2021; Zakrajšek et al., 2021; Campuzano-Bolarin et al., 2021; Povh in Žerovnik, 2021; Smole et al., 2021
2023	16	Nagy in Varga, 2023: Hladik, 2023; Gaspars-Wieloch, 2023; Perič et al., 2023; Garajova in Rada, 2023; Trazskalik, 2023; Gabrovšek et al., 2023; Čegovnik et al., 2023; Osz in Hegyhati, 2023; Lukać, 2023a; Lukać, 2023b; Milavec Kapun et al., 2023; Varga in Madari, 2023; Pejić Bach et al., 2023; Krpan, 2023; Kašparova, 2023

njihovo uporabo na različnih področjih, vključno z upravljanjem tveganj, matematičnim programiranjem, teorijo iger, gravitacijsko analizo, prostorsko analizo, logistiko, krožnim gospodarstvom, stalnimi izboljšavami, trajnostjo, elektronskim poslovanjem, napovedovanjem, Gaussovimi procesi, linearno regresijo, večplastnim zaznavanjem in strojnim učenjem. Avtorji so iz Portugalske (5), Hrvaške (3) in Slovenije (2).

Za BSR-SI, letnik 11, številka 2, leto 2020, je bilo izbranih enajst prispevkov, ki predstavljajo izboljšave in nove tehnike (metodologijo) OR ter njihovo uporabo na različnih področjih ekonomije, prostorskih ved, pametne mobilnosti, visokega šolstva, človeških virov, okolja, kmetijstva in družabnih omrežij. Avtorji teh prispevkov so iz Hrvaške (3), Slovenije (3), Madžarske (1), Portugalske (1) in Češke (1), dva prispevka pa so napisali avtorji iz različnih držav: ena skupina je bila iz Nizozemske, Slovenije in Španije, druga pa iz Norveške, Madžarske in Slovenije.

Devet člankov je prejelo pozitivno oceno za BSR-SI, letnik 9, številka 2, leto 2018. V njih so predstavljene izboljšave in nove metode v OR ter njihova uporaba na različnih področjih ekonomije, prostorske znanosti in ocenjevanja lokacij. Avtorji so iz Slovenije (3), Hrvaške (3), Norveške (1), Turčije (1), po en prispevek sta napisala avtorja iz Hrvaške in Republike Severne Makedonije, po en prispevek pa avtorja iz Hrvaške in Singapurja.

Za BSR-SI, letnik 7, številka 2, leto 2016, je bilo izbranih sedem prispevkov, ki obravnavajo tehnike OR, kot so metoda Intramax, energetska analiza, multivariatna analiza in DEA, ter njihovo uporabo na različnih področjih ekonomije. Avtorji so iz Hrvaške (4), Slovenije (2) in Češke (1).

Za BSR-SI, letnik 5, številka 3, leto 2014, je bilo izbranih šest člankov, ki obravnavajo probleme visokorazsežne klasifikacije z uporabo strojnega učenja, delniške trge z uporabo mer nelikvidnosti, optimizacijo informacijskih sistemov z uporabo LP, uporabo statističnih metod za uspešnost malih podjetij, metodo Intramax za preučevanje funkcionalnih regij in modele čakalnih vrst za optimizacijo delovanja klicnega centra. Štirje avtorji so iz Hrvaške in dva iz Slovenije. Trije avtorji iz Slovenije in trije iz Hrvaške so sodelovali pri prvi BSR-SI, ki jo je izdala SDI-SOR. Preučevali so dinamiko inflacije, uporabo gravitacijskega modela za primer delavcev, ki se vozijo na delo, teorijo večkriterijskih skupinskih modelov, analizo upravljanja na podlagi inovativnega statističnega pristopa, nevronske mreže in nove hevristike za reševanje problema pakiranja smeti.

SDI-SOR sodeluje tudi pri reviji Uporabna informatika (v slovenščini; angl.: Applied Informatics; https://uporabna-informatika.si/ui, slovenska revija za računalništvo/OR). Njeno poslanstvo je obveščanje strokovne javnosti in uporabnikov o najnovejših dosežkih na področju informatike/OR v Sloveniji in po svetu. Posebna odlika revije so informacije o slovenskih raziskovalnih projektih in evropskih dokumentih, ki so osnova za trende v informatiki/OR in neizogibno vplivajo na naše okolje.

Člani SDI-SOR aktivno sodelujemo kot avtorji člankov, recenzenti in člani uredniškega odbora pri CrORR (Croatian Operational Research Review, indeksirano v Wos ESCI). Aktivno sodelujemo kot avtorji člankov in recenzenti pri v reviji Multicriteria Decision Making, The University of Economics in Katowice, Poland (v letih 2013, 2014 …).

Leta 2011 je v Wiley Encyclopedia of Operations Research and Management Science, (urednik J. J. Cochran) izšlo poročilo o delu SDI-SOR (Zadnik Stirn, 2011).

7 SKLEPNE MISLI

OR so pomembno raziskovalno področje, saj s podporo OR dnevno izboljšujemo procese na vseh ravneh, kot na primer pri načrtovanje čakalnih vrst, optimizaciji dobavnih verig, telekomunikacijah ali pri odločitvah o načrtovanju virov. Z izboljšanjem procesov omogočamo višjo kakovost izdelkov in storitev, večje zadovoljstvo strank in boljše odločanje. Nobenega dvoma ni, da OR prispevajo h kakovosti življenja in gospodarski blaginji na mikroekonomski, makroekonomski in globalni ravni.

Da bi zagotovili ustrezne rešitve, tudi z obdelavo informacij, katerih obseg eksponentno narašča, kar je posledica hitrega razvoja tehnologije, je nenehno treba razvijati nove metode in modele OR. Inovativni modeli za podporo odločanju, modeli OR, so ključni za učinkovito spopadanje z globalnimi izzivi, kot so podnebne spremembe, učinkovita raba virov, večje zahteve po socialnem varstvu, selitve, posegi v infrastrukturo in naravo, spodbujanje gospodarske rasti, omejeni proračuni, s katerimi se spopadajo vlade (na primer Načrt za okrevanje in odpornost, RS GOV.SI, 2023) in družba kot celota.

Modeli OR so v zadnjih desetletjih posegli v vsa okolja ter spremenili načine in pristope sprejemanja odločitev. Spoznali smo prednosti, ki jih je mogoče

pridobiti z uporabo OR modelov/metod. Pionirke pri razvoju in uporabi OR so skandinavske države, Združeno kraljestvo, ZDA in v zadnjem času države Bližnjega vzhoda.

V modele in metode OR bo treba še intenzivneje vključevati novo nastajajoča področja, kot so na primer vedenjska ekonomija (Biloslavo et al., 2022), krožna ekonomija (Hojnik et al., 2022), življenjski cikel proizvodov (Lipušček et al., 2010). Intenzivneje bo treba izpostaviti tudi odnos odločevalcev do dejavnosti in interakcij z drugimi, to je razvijati pristope k skupinskemu odločanju (Kalech, 2021). Pri tem pa je seveda treba upoštevati osebnostne preference in čustva odločevalcev ob hkratnem odločanju v dobro širše skupnosti. Odločevalec mora odločati trajnostno in družbeno odgovorno. Imeti mora pozitiven odnos do družbe kot celote in narave/okolja, ob minimiziranju tveganja, nekonsistentnosti, pristranosti, poenostavljanja in spregledanja obstoječih informacij ter zavestnega ohranjanja obstoječega stanja, ki je lahko v korist samo odločevalcu ob hkratnem zanemarjanju dolgoročnega trajnostnega razvoja, kar ima običajno daljnosežne negativne posledice za vse. Nadalje pa OR zahtevajo timsko delo, intenzivno sodelovanje z odločevalci in tudi akterji (del družbe), na katerih življenje bo izbrana odločitev vplivala.

Čeprav je opus opravljenega dela članov SDI-SOR v več kot 30-letih obstoja sekcije OR izredno velik, ostaja še vrsto nalog, ki jih bo treba še opraviti. Izzivov je torej še mnogo:

- nadaljevanje sodelovanja SDI-SOR s FOV in FS UL ter intenziviranje tega sodelovanja s številnimi drugimi fakultetami (EF UL, EPF UM, UP …) in iskanje novih povezav v okviru fakultet, inštitutov in raziskovalnih organizacij;
- še naprej aktivno sodelovanje v mednarodnih zvezah IFORS, EURO, IFIP in drugimi ter prevzemanje vidnih funkcij v teh organizacijah;
- povezovanje s tujimi društvi OR (hrvaškim, avstrijskim, nemškim, češkim, madžarskim, slovaškim, poljskim, ameriškim in drugimi) ter iskanje novih povezav predvsem pri skupnih raziskovalnih projektih in pri objavljanju ter diseminaciji dosežkov (konference in druge oblike srečanj);
- predstavitev dela SDI-SOR v Wikipediji na strani EURO http://en.wikipedia.org/wiki/Association_of_European_Operational_Research_Societies;
- objava Zbornikov Proceedings SOR'93, …, SOR'03 (7) in vseh SDI-SOR monografij (4) v elektronski obliki in posledično njihova objava na spletni strani sekcije;
- imenovanje skupine prostovoljcev, ki bi se ukvarjali s terminologijo OR; osnova bi lahko bila publikacija Terminološki rečnik iz operacionih istraživanja (1983) in številni tuji terminološki slovarji;
- vključevanje OR v pedagoški proces na vseh stopnjah študija;
- seznanjanje gospodarskih subjektov in javnosti z možnostjo uporabe OR; povečanje števila članstva tudi preko vključevanja kolegov v skupne projekte in študentov preko diplomskih nalog, študentskih projektov in njihovega sodelovanja na srečanjih domačih in mednarodnih akterjev v okviru konferenc in drugih oblikah;
- tesnejše povezovanje znotraj SDI na različnih področjih: pri organizaciji, vodenju sekcij, predstavitvah prispevkov, okroglih mizah, delavnicah na DSI, pri delu na terminoloških slovarjih, skupnih znanstvenih projektih in promociji v javnosti;
- aktivno delovanje na področju publicistike, predvsem znanstvene preko domačih in tujih znanstvenih revij (nadaljevati s posebnimi številkami CEJOR, BSRJ in drugih revij).

Za svoje prispevke na področju informatike in OR so člani SDI-SOR prejeli tudi nagrade in priznanja, med njimi:

- Priznanje SDI za razvoj mednarodnega sodelovanja in izmenjavo dosežkov na področju OR - april 2007;
- Častno članstvo v OEGOR (Austrian Society of OR) - november 2018;
- Zlati častni znak SDI za življenjsko delo in promocijo SDI (SOR) v mednarodnem okolju - april 2019;
- Nagrada Donald Michie-Alan Turing za življenjsko delo na področju informacijsko-upravljavskih znanosti (informacijske družbe) - november 2020;
- Zlati častni znak SDI za obsežno raziskovalno in pedagoško delo na področju operacijskih raziskav in geoinformatike - maj 2022;
- Naziv Legende informatike in računalništva (Programski odbor IS 2023, IJS) - oktober 2023;
- Nagrado EDSA (EURO Distinguished Service Award) kot priznanje za delo v Evropskih združenjih OR (EURO - Union of European OR Societies), v svetu EURO, komisijah EURO in mednarodnih OR publikacijah – junij 2024.

8 ZAHVALA

Vseh teh dejavnosti člani SDI-SOR ne bi mogli izvesti brez podpore in odličnega sodelovanja s številnimi kolegi doma in v tujini. Tako se ob tej priložnosti zahvaljujemo:

- gospodu Niku Schlambergerju, dolgoletnemu predsedniku SDI za vso podporo, razumevanje, pomoč, ideje in vsestranskim držanjem dežnika, pod katerim SOR varno sobiva; sodelovanje z g. Schlambergerjem je bilo za SOR vsa leta zelo stimulativno;
- zaslužni prof. dr. Ulriki Leopold Wildburger (Univerza Graz) za povabilo in sodelovanje pri reviji CEJOR, pomoč in podporo pri organizaciji simpozijev v Sloveniji in številnih drugih mednarodnih dejavnostih;
- kolegom iz HDOI za dolgoletno sodelovanje in razumevanje pri izmenjavanju v organizaciji mednarodnih simpozijev, predvsem pa prvemu predsedniku prof. L. Neraliću za pomoč in podporo pri včlanjevanju SDI-SOR v IFORS;
- ustanoviteljem SDI-SOR, ki ste postavili temelje za delovanje sekcije doma in v tujini, in vsem številnim članom SDI-SOR, ki ste prostovoljno z veliko znanja, navdušenja in volje pripomogli k uspešnemu več kot 30-letnemu delu SDI-SOR.

9 LITERATURA

[1] Biloslavo, R., Edgar, D., Rusjan, R. (2022). Strategic dualities and business model innovation within SMEs. *Journal of East European management studies*, 27(3), 379–403. https://doi.org/10.5771/0949-6181-2022-3-462

[2] Bohanec M. (2012). *Odločanje in modeli*. Ljubljana: DMFA.

[3] Boucherie, R. J., van Dijk, N. M. (2017). *Markov decision processes in practice*, Springer.

[4] Bouyssou, D., Marchant, T., Pirlot, M. (2006). *Evaluation and Decision Models with Multiple Criteria*; Steppingstone for the Analyst. New York: Springer.

[5] Bronson, R., Naadimuthu, G. (1997). *Schaum's Outline of Operations Research*. McGraw Hill.

[6] Charnes, A. (1952). Optimality and degeneracy in linear programming. *Econometrica*, 20, 160–170. https://doi.org/10.2307/1907845

[7] Charnes, A., Cooper, W. W., Rhodes, E. (1978). Measuring the efficiency of decision-making units. *European Journal of Operational Research*, 2, 429–444. https://doi.org/10.1016/0377-2217(78)90138-8

[8] Curwin, J., Slater, R. (2013). *Quantitative methods for business decisions. Cengage Learning*.

[9] Dantzig, G. B. (1951). *Application of the simplex method to a transportation problem, v Activity analysis of production and allocation*, Koopmanns T. C., ur., New York: John Wiley, str. 359–373.

[10] Dantzig, G.B. (1963). *Linear programming and extensions. New Jersey: Princeton.*

[11] Drobne, S., Zadnik Stirn, L., Žmuk, B. (2022). Editorial for the Special Issue: Novel Solutions and Novel Approaches in Operational Research. Business Systems Research, 13(3), 1–7.

[12] Gal, T., Horst, R. Isermann, H., Mueller-Merbach, H. (1991). *Grundlagen des Operations Research*, Berlin: Springer.

[13] Hillier, F. S., Liebermann, G. J. (2020). *Introduction to Operations Research*. McGraw-Hill.

[14] Hojnik, J., Biloslavo, R. Bertoncel, T. (2022). Business model for a circular economy: a literature review with bibliometric and topic analysis. V Business models for the circular economy: a European perspective, Prokop, V. et al., ur., Springer, str. 13–64, *Sustainability and innovation*. http://dx.doi.org/10.1007/978-3-031-08313-6_2

[15] Ishizaka, A., Nemery, P. (2013). Multi-Criteria Decision Analysis. John Wiley.

[16] Ittmann, H. (2008). Welcome to a new IFORS member society. IFORS news, 2/3(Sept.), str. 8–10.

[17] Jablonsky, J., Černy, M., Pekar, J. (2022). The last dozen of years of OR research in Czechia and Slovakia. Central European Journal of Operations Research, 30(2), 435–447. https://doi.org/10.1007/s10100-022-00795-4.

[18] Joergensen, S. E., Fath, B. D. (2011). Fundamentals of Ecological Modelling: Applications in Environmental Management and Research. Amsterdam: Elsevier.

[19] Jones, D., Tamiz, M. (2010). Practical goal programming. International Series in Operations Research and Management Science. New York: Springer.

[20] Kalech, M. (2021). Decision-Making under Group Commitment. Mathematics 9(17), 2080. http://dx.doi.org/10.3390/math9172080

[21] Kant, S., Berry, R. A. (2005). Economics, Sustainability and Natural Resources: Economics of Multiple Forest Use. Dordrecht: Springer.

[22] Kantorovič, L. V. (1939). Matematičeskie metody v organizacii i planirovanii proizvodstva. LGU.

[23] Kantorovič, L. V. (1959). Ekonomičeskij rasčot najlučšego ispolzovanija resursov. AN, SSSR.

[24] Karush, W. (1939). Minima of Functions of Several Variables with Inequalities as Side Constraints (Thesis). M.Sc. Dissertation. Dept. of Mathematics, Univ. of Chicago, Chicago, Illinois. https://catalog.lib.uchicago.edu/vufind/Record/4111654

[25] Kastrin, A., Povh, J., Zadnik Stirn, L., Žerovnik J. (2021). Methodologies and applications for resilient global development from the aspect of SDI-SOR special issues of CJOR. Central European Journal of Operations Research, 29(3): 773–790. https://doi.org/10.1007/s10100-021-00752-7.

[26] Kuhn, H. W. (1976). Nonlinear programming: a historical view, V Nonlinear programming, SIAM-AMS Proceedings, Cottle, R. W., Lemke, C. E., ur., Rhode Island: Providence.

[27] Lipušček, I., Bohanec, M., Oblak, L., Zadnik Stirn, L. (2010). A multi-criteria decision-making model for classifying wood products with respect to their impact on environment. The international journal of life cycle assessment, 15(4), 359–367. http://dx.doi.org/10.1007/s11367-010-0157-6

[28] Lukač, Z., Neralić, L. (2012). Operacijska istraživanja. Zagreb: Element.

[29] Povh, J., Zadnik Stirn, L., Žerovnik, J. (2023). 60 years of OR in Slovenia: development from first conference to a vibrant community. Central European Journal of Operations Research, 31(3), 681–690. https://doi.org/10.1007/s10100-023-00859-z

[30] Powell, S. G., Baker, K. R. (2010). Management science: The art of modeling with spreadsheets. Wiley.

[31] RS GOV.SI (2023). Načrt za okrevanje in odpornost. Republika Slovenija GOV.SI. Urad Republike Slovenije za okrevanje

in odpornost. https://www.gov.si/zbirke/projekti-in-programi/nacrt-za-okrevanje-in-odpornost/
[32] Pukkala, T. (2002). Multiobjective forest planning. London: Kluwer.
[33] Ragsadale, C. T. (2010). Spreadsheet Modeling & decision analysis. Edition 6.
[34] Rupnik, V. (1974). Oris operacijskih raziskav. Kranj: Moderna organizacija.
[35] Rupnik, V. (1998). Teorija faktorjev integrabilnosti gospodarstva in njihovo praktično modeliranje. Ljubljana: Slovenian Society Informatika – Section of Operations Research.
[36] Rupnik, V. (2013). Globalizacijski izzivi. Ljubljana: Slovenian Society Informatika – Section of Operations Research.
[37] Rupnik, V., Sundać, D. (2005). Dominacija kapitala = Past človeštvu, Rijeka: I.B.B.C.
[38] Rupnik, V., Zadnik Stirn, L., Drobne, S., ur. (2000). Rešeni problemi proizvodnje/Solutions to Production Problems. Ljubljana: Slovenian Society Informatika – Section of Operations Research.
[39] Saaty, T. L. (2006). Fundamentals of Decision Making and priority theory with the Analytic Hierarchy Process. RWS Publications.
[40] Salaff, S. (1972). A biography of Hua Lo-Keng. Isios, 63, 142–183.
[41] SYM-OP-IS'86 (1986). Zbornik radova XIII jugoslovenskog simpozija operacionih istraživanja, Herceg Novi, 7-10 oktobar, Beograd: Fakultet organizacionih nauka.
[42] Terminološki rečnik iz operacionih istraživanja, 1983. SYM-OP-IS'83, Beograd: Fakultet organizacionih nauka.
[43] Weintraub, A., Romero, C., Bjorndal, T., Epstein, R. (2007). Handbook of Operations Research in natural resources. Springer.
[44] Winston, W. L. (2005). Operations research, application, and algorithms. Belmont: Thomson Learning.
[45] Zadnik Stirn, L. (2001). Metode operacijskih raziskav za poz slovno odločanje. Novo mesto: Visoka šola za upravljanje in poslovanje.
[46] Zadnik Stirn, L. (2002). O delu SDI-SOR v letih 1997-2002, Slovensko društvo Informatika - Sekcija za operacijske raziskave, https://www.drustvo-informatika.si/sekcije-drustva
[47] Zadnik Stirn, L. (2011). Slovenian Society Informatika (SSI) – Section for Operations Research (SOR). Wiley Encyclopaedia of Operations Research and Management Science, Cochran, J., ur., New Jersey: John Wiley and Sons, str. 5024-5029.
[48] Zadnik Stirn, L., Drobne, S. (2022). Ob 30-letnici sekcije SOR, (1992-2022), Ljubljana: Slovensko društvo Informatika - Sekcija za Operacijske raziskave. https://www.drustvo-informatika.si/sekcije-drustva.
[49] Zadnik Stirn, L., Ferbar, L., Indihar Štemberger, M., Drobne, S., ur. (2005). Selected Decision Support Models for Production and Public Policy Problems. Ljubljana: Slovenian Society Informatika – Section of Operations Research.
[50] Zadnik Stirn, L., Grošelj, P. (2019). Keeping Slovenia green: How to best manage famed forest region. OR/MS today. March 25. https://doi.org/10.1287/orms.2019.02.10
[51] Zbornik, 1964. Mehanografija in operacijsko raziskovanje. Ljubljana: Cankarjeva založba.
[52] Zbornik, 1967. Posvetovanje o uporabi metod OR v delovnih organizacijah v Jugoslaviji. Ljubljana: Društvo ekonomistov Ljubljana, Zavod Magistrat.
[53] Proceedings of the International Symposium on Operational Research SOR
[54] Drobne, S., Zadnik Stirn, L., Kljajić Borštnar, M., Povh, J., ŽerovŽ nik, J., ur. (2023). Proceedings of the 17th International Sympoa sium on Operational Research SOR'23. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor
[55] Drobne, S., Zadnik Stirn, L., Kljajić Borštnar, M., Povh, J., Žerovnik, J., ur. (2021). Proceedings of the 16th International Symposium on Operational Research SOR'21. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=-publikacije-sor
[56] Drobne, S., Zadnik Stirn, L., Kljajić Borštnar, M., Povh, J., Žerovnik, J., ur. (2019). Proceedings of the 15th International Symposium on Operational Research SOR'19. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=-publikacije-sor
[57] Zadnik Stirn, L., Kljajić Borštnar, M., Žerovnik, J., Drobne, S., ur., (2017). Proceedings of the 14th International Symposium on Operational Research SOR'17. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor
[58] Zadnik Stirn, L., Žerovnik, J., Kljajić Borštnar, M., Drobne, S., ur. (2015). Proceedings of the 13th International Symposium on Operational Research SOR'15. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor
[59] Zadnik Stirn, L., Žerovnik, J., Povh, J., Drobne, S.., Lisec, A., ur. (2013). Proceedings of the 12th International Symposium on Operational Research SOR'13. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor
[60] Zadnik Stirn, L., Žerovnik, J., Povh, J., Drobne, S.., Lisec, A., ur. (2011). Proceedings of the 11th International Symposium on Operational Research SOR'11. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor
[61] Zadnik Stirn, L., Žerovnik, J., Drobne, S.., Lisec, A., ur. (2009). Proceedings of the 10th International Symposium on Operational Research SOR'09. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor
[62] Zadnik Stirn, L., Drobne, S., ur. (2007). Proceedings of the 9th International Symposium on Operational Research SOR'07. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor
[63] Zadnik Stirn, L., Drobne, S., ur. (2005). Proceedings of the 8th International Symposium on Operational Research SOR'05. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor
[64] Zadnik Stirn, L., Bastič, M., Drobne, S., ur. (2003). Proceer dings of the 7th International Symposium on Operational Research SOR'03. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor
[65] Lenart, L., Zadnik Stirn, L., Drobne, S., ur. (2001). Proceer dings of the 6th International Symposium on Operational Research SOR'01. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor
[66] Rupnik, V., Zadnik Stirn, L., Drobne, S., ur. (1999). Proceer dings of the 5th International Symposium on Operational Research SOR'99. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije-drustva?stran=publikacije-sor

[67] Rupnik, V., Zadnik Stirn, L., Drobne, S., ur. (1997). Proceer dings of the 4th International Symposium on Operational Research SOR'97. Ljubljana: Slovenian Society Informatika. https://www.drustvo-informatika.si/sekcije-drustva?stran=-publikacije-sor

[68] Rupnik, V., Bogataj, M., ur. (1995). Proceedings of the 3th International Symposium on Operational Research SOR'95. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije--drustva?stran=publikacije-sor

[69] Rupnik, V., Bogataj, M., ur. (1994). Proceedings of the 2th International Symposium on Operational Research SOR'94. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije--drustva?stran=publikacije-sor.

[70] Rupnik, V., Bogataj, L., ur. (1993). Proceedings of the 1th International Symposium on Operational Research SOR'93. Ljubljana: Slovenian Society Informatika – Section of Operations Research. https://www.drustvo-informatika.si/sekcije--drustva?stran=publikacije-sor.

▪

Lidija Zadnik Stirn je zaslužna profesorica za področje Operacijske raziskave na Univerzi v Ljubljani, Biotehniška fakulteta in izredna profesorica na Univerzi Tennessee, Knoxville, ZDA. Raziskovalno je usmerjena predvsem v deterministične, stohastične, dinamične, večkriterijske in skupinske metode odločanja za socioekonomske in ekološke probleme upravljanja z naravnimi viri. Njeno raziskovalno, predvsem mednarodno, in pedagoško delo rezultirata v več kot 600 objavah. Od leta 1997 je predsednica Sekcije za operacijske raziskave (SDI-SOR), v letih 2002-2023 je bila podpredsednica Slovenskega društva INFORMATIKA (SDI), je slovenska predstavnica v IFORS, EURO in IFIP TC7 ter koordinatorka IUFRO skupine upravljavska ekonomika.

▪

Samo Drobne je izredni profesor za področje Geodezija in geoinformatika na Univerzi v Ljubljani, Fakulteti za gradbeništvo in geodezijo. Raziskovalno se ukvarja predvsem s prostorskimi analizami oz. prostorsko statistiko v geografskih informacijskih sistemih ter s prostorski sistemi oz. uporabo operacijskih raziskav v prostoru, s posebnim poudarkom na prostorskih interakcijskih modelih in funkcionalnih regijah. Njegovo raziskovalno, strokovno in pedagoško delo rezultira v več kot 700 objavah. Od leta 1992 je tajnik Sekcije za operacijske raziskave, v okviru Slovenskega društva INFORMATIKA (SDI-SOR).

.

Uporaba podatkovnih prostorov na primeru izmenjave podatkov med mestno občino Celje in portalom Odprti podatki o Sloveniji

Ruben Ferreira[1], Erazem Stanonik[1], Jana Volk[1], Alen Cigler[1], Hana Skitek[1]
[1]Fakulteta za računalništvo in informatiko, Večna pot 113, 1000 Ljubljana rf5885@student.uni-lj.si, es0402@student.uni-lj.si, jv0719@student.uni-lj.si, ac2360@student.uni-lj.si, hs8668@student.uni-lj.si

Izvleček

Podatkovni prostori predstavljajo inovativno rešitev za varno, decentralizirano in suvereno izmenjavo podatkov med organizacijami. Glavna prednost je nadzor lastnikov podatkov nad dostopom in pogoji deljenja, kar zmanjšuje tveganje kibernetskih napadov in zlorab. Uvedba standardov, kot je International Data Spaces (IDS), omogoča enotno in zanesljivo izmenjavo podatkov v različnih sektorjih, kot so zdravstvo, industrija in javna uprava. Evropske iniciative, kot sta GAIA-X in Evropska strategija za podatke, podpirajo vzpostavitev enotnega trga za podatke. Praktični primer implementacije med Mestno občino Celje in portalom Odprti podatki Slovenije prikazuje izboljšanje učinkovitosti javnih storitev in varnosti podatkov. Podatkovni prostori tako predstavljajo ključen element digitalne transformacije, ki spodbuja inovacije, rast in trajnostni razvoj s poudarkom na varnosti in suverenosti podatkov.

Ključne besede: DS standard, podatkovni prostori, suverenost podatkov, varna izmenjava podatkov

Applicability of Data Spaces: the case Study of Data exchange between the Municipality of Celje and the Open Data Portal of Slovenia

Abstract

Data spaces represent an innovative solution for secure, decentralized, and sovereign data exchange among organizations. A key advantage is the control data owners have over access and sharing conditions, reducing the risk of cyber-attacks and data misuse. The introduction of standards such as International Data Spaces (IDS) enables uniform and reliable data exchange across various sectors, e.g., healthcare, industry, and public administration. European initiatives, such as GAIA-X and the European Data Strategy, support the establishment of a unified data market. A practical implementation example between the Municipality of Celje and the Open Data Portal of Slovenia demonstrates improved efficiency of public services and data security. Data spaces thus constitute a crucial element of digital transformation, promoting innovation, growth, and sustainable development with an emphasis on data security and sovereignty.

Keywords: IDS standard, data spaces, data sovereignty, secure data exchange

1 UVOD

Podatkovni prostori so nova, razvijajoča se rešitev na področju izmenjave podatkov. Dandanes podjetja med sabo delijo podatke na različne načine, z uporabo številnih standardov za njihovo izmenjavo. Podatkovni prostori predstavljajo napredno rešitev z IDS (International Data Spaces) standardom. Ta uvaja enoten, suveren in varen način izmenjave podatkov. Glavna prednost je decentralizirano shranjevanje ter deljenje podatkov. Tako so podatki vedno

pri lastniku, ta pa lahko nadzira komu deli dostop do njih in pod kakšnimi pogoji. S tem se zmanjša tveganje kibernetskih napadov ter zlorab podatkov, kar je v razvijajočem se digitalnem svetu vse pomembneje. Koncept podatkovnih prostorov je uporaben na mnogih področjih, ki bodo tekom članka tudi predstavljena. Prav tako bo naveden primer implementacije podatkovnega prostora v javni upravi - deljenje podatkov o parkirnih mestih v mestni občini Celje s portalom Odprti podatki Slovenije. Tako je pokazano, kako bi se lahko vse občine povezale na ta podatkovni prostor ter bi delile podatke s portalom, kar med drugim spodbudi ažurnost podatkov, saj jih ni treba ročno prepisovati.

2. PODATKOVNI PROSTORI

Podatkovni prostori, kot jih opredeljuje delovni dokument Evropske komisije o skupnih evropskih podatkovnih prostorih [3], združujejo relevantne podatkovne infrastrukture in okvire upravljanja, da bi omogočili združevanje in deljenje podatkov. Ta dokument prav tako določa značilnosti skupnega evropskega podatkovnega prostora, ki so:

Varnostna in zasebna infrastruktura za združevanje, dostopanje, deljenje, obdelovanje in uporabo podatkov.

Jasna in praktična struktura za pravičen in pregleden dostop do podatkov ter njihovo uporabo, ob tem pa jasni in zanesljivi mehanizmi upravljanja podatkov.

Popolno spoštovanje evropskih pravil in vrednot, predvsem varstva osebnih podatkov, zakonodaje o varstvu potrošnikov in konkurenčnega prava.

Imetniki podatkov bodo imeli možnost, da v podatkovnem prostoru odobrijo dostop do določenih osebnih ali neosebnih podatkov pod njihovim nadzorom ali jih delijo.

Podatki, ki so na voljo, se lahko ponovno uporabijo plačljivo ali brezplačno.

Sodelovanje odprtega števila organizacij/posameznikov.

Skupni evropski podatkovni prostori naj bi sledili posebnim načelom oblikovanja, ki vključujejo skupno tehnično infrastrukturo in gradnike ter povezljivost in interoperabilnost.

Podatkovni prostori naj bi po knjigi »Designing Data Spaces: The Ecosystem Approach to Competitive Advantage« [9] prispevali k pospeševanju digitalne preobrazbe znotraj in med različnimi področji ter podpirali gospodarske načrte za okrevanje. V prihodnosti je cilj imeti evropski podatkovni prostor, ki povezuje različne podatkovne prostore in zagotavlja, da se podatki obsežno delijo in uporabljajo ob spoštovanju vrednot in predpisov EU.

2.1 Pregled sektorjev podatkovnih prostorov

Podatkovni prostori so specializirani za različne sektorje [10], da bi izpolnili specifične potrebe in cilje vsakega sektorja. Sektorji so prikazani na sliki 1. Ti prostori omogočajo ciljno usmerjeno zbiranje, upravljanje in deljenje podatkov, kar spodbuja učinkovitost, inovacije in boljše odločitve. Vsak sektor podatkovnih prostorov ima svoje edinstvene zahteve glede varnosti, interoperabilnosti in regulacije, kar zahteva prilagojene rešitve.

- Zdravstveni podatkovni prostor: Namenjen je olajšanju izmenjave zdravstvenih podatkov med državami članicami, zdravstvenimi ustanovami in raziskovalci.
- Industrijski podatkovni prostor: Osredotoča se na industrijske podatke za povečanje učinkovitosti in inovacij v proizvodnih procesih.
- Podatkovni prostor mobilnosti: Povezuje podatke o prometu in mobilnosti za razvoj pametnejših in bolj trajnostnih transportnih rešitev.
- Energetski podatkovni prostor: Namenjen je izmenjavi podatkov o energiji za podporo trajnostnim energetskim sistemom.
- Kmetijski podatkovni prostor: Osredotoča se na kmetijske podatke za izboljšanje učinkovitosti in trajnosti kmetijske proizvodnje.
- Finančni podatkovni prostor: Povezuje finančne podatke za izboljšanje finančnih storitev in regulacije.
- Podatkovni prostor za zeleni dogovor: Podpira cilje evropskega zelenega dogovora z izmenjavo podatkov o okoljskih vplivih, trajnosti in podnebnih spremembah.
- Podatkovni prostor javne uprave: Namenjen je izboljšanju javnih storitev in upravljanja z izmenjavo podatkov med javnimi organi.
- Podatkovni prostor pametnih mest: Povezuje podatke za razvoj pametnih mest, vključno s podatki o infrastrukturi, transportu, energiji, komunikacijah in storitvah za državljane.
- Turistični podatkovni prostor: Namenjen je spodbujanju turizma z izmenjavo podatkov o turističnih destinacijah, storitvah, infrastrukturi in obiskovalcih.

- Podatkovni prostor kulturne dediščine: Osredotoča se na digitalizacijo in deljenje podatkov o kulturni dediščini.
- Medijski podatkovni prostor: Povezuje podatke iz medijskega sektorja za izboljšanje medijskih storitev, dostopa do informacij in inovacij v novinarstvu.
- Jezikovni podatkovni prostor: Namenjen je podpori jezikovnih tehnologij in večjezičnosti z izmenjavo jezikovnih podatkov.

2.2 Najpomembnejše iniciative in standardi za podatkovne prostore

V Evropi je bilo vzpostavljenih več iniciativ in standardov za podporo in razvoj podatkovnih prostorov, ki zagotavljajo varno, učinkovito in interoperabilno izmenjavo podatkov med različnimi sektorji. Med najpomembnejšimi so:

2.2.1 Evropska strategija za podatke

Evropska strategija za podatke [1] je zasnovana tako, da EU postane vodilna v podatkovno usmerjeni družbi. Glavni cilji strategije vključujejo ustvarjanje enotnega trga za podatke. To bo omogočilo prost pretok podatkov znotraj EU in med različnimi sektorji in s tem bo koristilo podjetjem, raziskovalcem in javnim upravam ter spodbudilo inovacije in rast.

2.2.2 Evropski akt o upravljanju podatkov (DGA)

Evropski akt o upravljanju podatkov (DGA) [2] je zakonodajna pobuda Evropske komisije, namenjena povečanju razpoložljivosti podatkov in krepitvi zaupanja v deljenje podatkov po celotni EU. Predlog zakona je bil predstavljen 25. novembra 2020 in je začel veljati 24. septembra 2023. DGA je pomemben del evropske strategije za podatke.

2.2.3 International Data Spaces (IDS)

International Data Spaces (IDS) [5] je ena izmed najpomembnejših iniciativ, ki omogoča varno in zaupanja vredno izmenjavo podatkov med podjetji in organizacijami. IDS ponuja referenčno arhitekturo, ki temelji na principih decentralizacije, suverenosti podatkov in interoperabilnosti. IDS zagotavlja, da lahko organizacije ohranijo popoln nadzor nad svojimi podatki ter hkrati omogočajo varno in pravno skladno deljenje teh podatkov z drugimi deležniki.

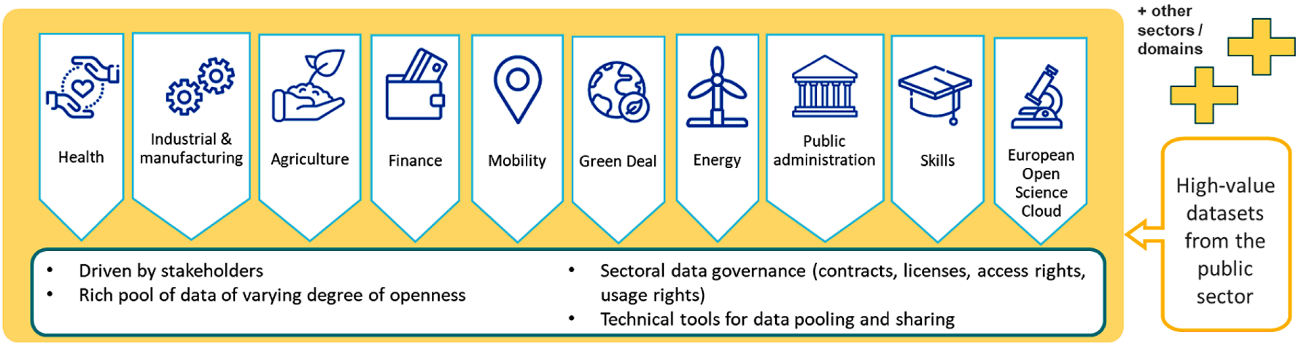
2.2.4 GAIA-X

GAIA-X [4] je evropska pobuda za vzpostavitev odprte in pregledne infrastrukture za podatke in oblačne storitve. Projekt si prizadeva za inovacije s pomočjo digitalne suverenosti, kar pomeni, da uporabniki obdržijo nadzor nad svojimi podatki. Gaia-X ne bo zgolj oblak, temveč federativni sistem, ki povezuje številne ponudnike storitev v oblaku in uporabnike v preglednem okolju, kar bo spodbudilo evropsko podatkovno ekonomijo prihodnosti.

3 POTREBA PO STANDARDIZACIJI PRENAŠANJA PODATKOV

3.1 Zakaj so podatkovni prostori potrebni?

V današnjem digitalnem svetu je deljenje podatkov med organizacijami postalo pomembno za učinkovito delovanje in sodelovanje. Podatki se v velikih količinah delijo v mnogo strokah industrije ter znanosti, med organizacijami vseh vrst. To deljenje podatkov pa je lahko problematično, saj imajo organizacije velikokrat različne ter svojevrstne načine, kako do njihovih podatkov dostopati, učenje teh načinov dostopa pa je lahko zamudno in neučinkovito. Poleg tega



Slika 1: **Sektorji evropskih podatkovnih prostorov. [10]**

so izmenjave podatkov danes velikokrat vprašljive varnosti, saj lahko pride do nepooblaščenega dostopa, izgube podatkov ali kibernetskih napadov. Tukaj nastopijo podatkovni prostori, ki omogočajo varen in standardiziran način izmenjave podatkov, kar povečuje zaupanje med partnerji in omogoča boljšo interoperabilnost. IDS (International Data Spaces) standard zagotavlja, da so podatki med deljenjem zaščiteni pred nepooblaščenim dostopom in da se delijo v skladu s pravili in regulativami.

3.2 International Data Spaces (IDS)

International Data Spaces (IDS) je standard, razvit za varno in suvereno izmenjavo podatkov med organizacijami. IDS zagotavlja, da se podatki delijo v skladu z določenimi pravili in predpisi. To pomeni da upošteva varnostne protokole, certifikacijo in upravljanje. Standard omogoča podjetjem, da izmenjujejo podatke brez strahu pred nepooblaščenim dostopom ali zlorabo, s čimer se povečuje zaupanje med sodelujočimi partnerji.

Glavne komponente IDS-ja so:

- IDS Connector[6]: je osrednja komponenta v ekosistemu podatkovnih prostorov, ki omogoča povezavo obstoječih sistemov in njihovih podatkov z IDS ekosistemom. Deluje kot vrata za vstop v podatkovne prostore, kjer se podatki izmenjujejo varno in v skladu s standardi IDS.
- IDS Broker: Posrednik, ki upravlja metapodatke o razpoložljivih podatkovnih virih v ekosistemu IDS. Omogoča iskanje in dostop do podatkov različnih ponudnikov.
- IDS Clearing House: Posrednik, ki zagotavlja storitve za poravnavo in poročanje o transakcijah izmenjave podatkov. Omogoča zanesljivo in pregledno sledenje podatkovnim transakcijam.
- IDS App Store: Trgovina z aplikacijami, kjer lahko ponudniki aplikacij objavijo in delijo aplikacije za obdelavo podatkov znotraj IDS ekosistema.
- IDS Identity Provider: Ponudnik identitet, ki upravlja in preverja identiteto udeležencev v IDS. Zagotavlja varnost in zaupanje v ekosistemu. Sestoji iz Certifikatne agencije (CA) za izdajo X.509 certifikatov in Dinamične storitve zagotavljanja atributov (DAPS) za upravljanje dinamičnih atributov in dostopnih žetonov.

Namen IDS-ja, kot ga definira International Data Spaces Association (IDSA) [7], je vzpostaviti zaupanje med udeleženci podatkovnih prostorov skozi stroge varnostne ukrepe in certifikacijo. To vključuje naslednje komponente:

- Zaupanje: Vsak udeleženec je ocenjen in certificiran pred pridružitvijo ekosistemu IDS, kar zagotavlja visoko raven zaupanja.
- Varnost in suverenost podatkov: Vsi deli IDS uporabljajo najsodobnejše varnostne ukrepe. Lastniki podatkov lahko določijo omejitve uporabe, ki jih morajo prejemniki podatkov spoštovati.
- Ekosistem podatkov: IDS spodbuja decentralizirano shranjevanje podatkov, kar pomeni, da podatki ostanejo pri lastniku do prenosa na zaupanja vredno stranko.
- Standardizirana interoperabilnost: IDS Connector omogoča komunikacijo med različnimi ponu- dniki in prejemniki podatkov znotraj ekosistema IDS.
- Aplikacije z dodano vrednostjo: IDS omogoča uporabo aplikacij za obdelavo podatkov, ki zagotavljajo dodatne storitve, kot so analiza podatkov, prilagoditev podatkovnih formatov in drugi procesi.
- Trgi podatkov: IDS omogoča nastanek novih podatkovno vodenih storitev in poslovnih modelov s podporo za trge podatkov in mehanizme za obračunavanje ter poravnavo.

Implementacija podatkovnih prostorov po standardu IDS omogoča učinkovito zbiranje, obdelavo in deljenje podatkov med različnimi entitetami. S tem se povečuje interoperabilnost, varnost podatkov in zaupanje med sodelujočimi organizacijami, kar prispeva k boljši uporabi javnih podatkov za razvoj aplikacij in storitev z dodano vrednostjo. Podatkovni prostori omogočajo centralizirano in varno upravljanje podatkov, kar olajša dostop do kakovostnih in zanesljivih podatkov za vse deležnike, ki jih potrebujejo za svoje delovanje.

3.3 Minimum Viable Data Space (MVDS)

Minimum Viable Data Space (MVDS) je različica IDS-ja, ki vsebuje minimalno število komponent, tako da omogočajo vzpostavitev podatkovnega prostora z zadostnim številom funkcij za varno in suvereno izmenjavo podatkov, kot je določeno s strani IDSA. Namen MVDS je olajšati delo razvijalcem s skrajšanjem časa implementacije, kar omogoča hitro vzpostavitev prve delujoče različice. Potrebne komponente za vzpostavitev MVDS-ja sta IDS Connector in IDS Identity Provider, opisana v oddelku 3.2.

4 PRIMER IMPLEMENTACIJE: PODATKOVNI PROSTOR MOC-OPSI

4.1 Podatkovni prostori v javni upravi

Kot omenjeno v predelu 2.1, so podatkovni prostori uporabni tudi v javni upravi. V okviru tega projekta se osredotočamo na dve specifični organizaciji - Mestna Občina Celje (MOC) in Odprti podatki Slovenije (OPSI). Pokažemo, kako implementacija podatkovnih prostorov po standardu IDS optimizira njune aktivnosti in povečuje varnost poslovanja.

4.2 Mestna Občina Celje (MOC)

Mestna občina Celje (MOC) je ena izmed regionalnih uprav Slovenije, ki je odgovorna za upravljanje mesta Celje in okoliških območij. Njene poslovne dejavnosti vključujejo:

- Urbano načrtovanje in razvoj: Upravljanje prostorskih načrtov, razvoj infrastrukture, stanovanjske politike in drugih urbanih projektov.
- Javne storitve: Zagotavljanje storitev, kot so vzdrževanje javnih površin, odvoz odpadkov, javni prevoz in druge komunalne storitve.
- Socialne storitve: Pomoč ranljivim skupinam prebivalstva, socialno varstvo, izobraževanje in kulturne dejavnosti.
- Okoljevarstvo: Upravljanje naravnih virov, nadzor nad onesnaževanjem, varstvo naravnih območij in spodbujanje trajnostnega razvoja.

Pomen dobrega upravljanja s podatki za MOC

Za učinkovito izvajanje teh dejavnosti je pomembno dobro upravljanje podatkov. Natančni in dostopni podatki omogočajo MOC boljše načrtovanje in izvajanje politik, hitrejše in boljše odločanje ter učinkovitejšo komunikacijo z javnostjo. Nekateri specifični vidiki, kjer dobro upravljanje podatkov igra vlogo, vključujejo:

Urbano načrtovanje in razvoj: Dostop do ažurnih in natančnih podatkov o zemljiščih, stavbah in infrastrukturi je bistven za učinkovito prostorsko načrtovanje in razvoj mestnih območij.

Javne storitve: Optimizacija storitev, kot so zbiranje odpadkov in vzdrževanje infrastrukture, zahteva natančne podatke o trenutnem stanju in potrebah prebivalcev.

Socialne storitve: Prilagajanje socialnih storitev potrebam prebivalstva temelji na podrobnih demografskih podatkih in podatkih o uporabi storitev.

Okoljevarstvo: Spremljanje in upravljanje okoljskih podatkov, kot so kakovost zraka, voda in ravnanje z odpadki, je ključno za trajnostno upravljanje naravnih virov.

4.3 Odprti podatki Slovenije (OPSI)

Portal odprtih podatkov Slovenije (OPSI) [8] je vzpostavilo Ministrstvo za javno upravo na odprtokodni programski opremi, z namenom zagotoviti enotno nacionalno točko za objavo odprtih podatkov javnega sektorja. Portal omogoča dostop do metapodatkov in zbirk podatkov, ki jih vodijo državni organi, občine in drugi javni organi.

OPSI vključuje centralni katalog evidenc in zbirk podatkov, ki omogoča dostop do metapodatkovnih opisov vseh zbirk javnega sektorja. Podatki so objavljeni pod odprto licenco, kar omogoča njihovo prosto uporabo za različne namene.

Standardizacija deljenja teh podatkov, dostopnih preko OPSI, bi naredila ta proces veliko bolj učinkovit, podatke lažje dostopne publiki ter bi zvišala varnost pri deljenju. Poleg tega bi bil OPSI odgovoren le za deljenje teh podatkov od lastnika do porabnika, saj IDS narekuje decentralizacijo podatkov, kjer le ti ostanejo pri lastniku do same izmenjave.

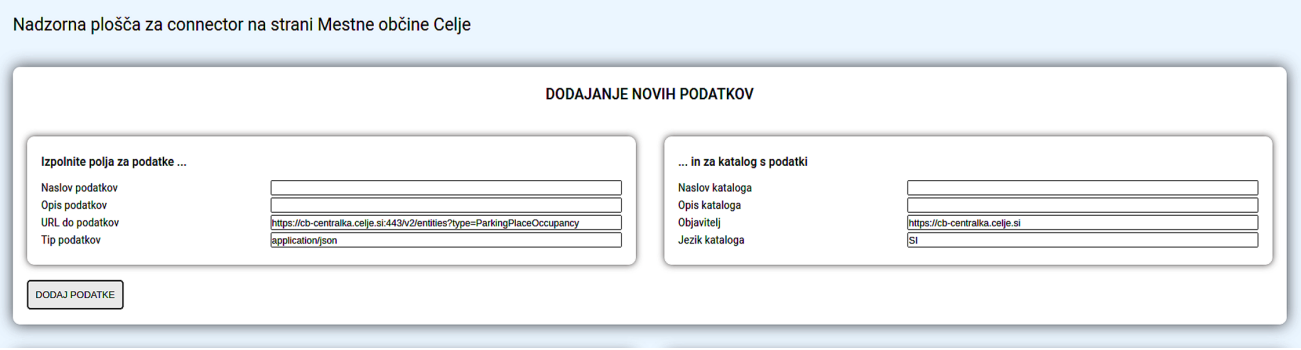
4.4 Konkretna implementacija MVDS

Projekt je zajemal vzpostavitev Minimal Viable Data Space (MVDS) med Mestno občino Celje (MOC) in portalom OPSI. Cilj je bil ustvariti varen in učinkovit sistem za izmenjavo podatkov, ki bi ustrezal standardom IDS in potrebam obeh organizacij. V nadaljevanju so predstavljeni konkretni koraki implementacije, izzivi, s katerimi smo se soočali, in komponente, ki smo jih razvili.

4.4.1 Koraki implementacije

Implementacija se je začela s analizo potreb MOC in OPSI ter podrobnim pregledom IDS standardov. To je omogočilo jasno razumevanje ciljev in tehničnih zahtev projekta. Nato se je vzpostavilo razvojno okolje z uporabo IDS Testbed za simulacijo MVDS, kar je vključevalo namestitev in konfiguracijo Docker kontejnerjev za različne komponente IDS.

Pri implementaciji MOC konektorja so se razvile Python skripte za učinkovito komunikacijo s context brokerjem MOC, ki so služile za avtomatizirano postavitev okolja. Vzporedno se je implementiral REST API za dostop do podatkov preko konektorjev in in-



Slika 2: **Nadzorna Plošča MOC**

tegriralo IDS protokole za zagotavljanje varne komunikacije. OPSI konektor se je zasnoval tako, da lahko učinkovito komunicira z MOC konektorjem in hkrati upravlja s prejetimi podatki.

Implementirali smo podporo za dnevno osvežene podatke, kot tudi podatke v realnem času. Uporabniki lahko tako izbirajo med dnevno posodobljenimi podatki, ki so primerni za splošne analize in načrtovanje, ter podatki v realnem času, ki omogočajo sprejemanje trenutnih odločitev. Za dnevno osvežene smo uporabili integracijsko orodje Apache Camel, ki je preko Cron komponente periodično pridobival podatke iz MOC in jih shranjeval na konektorju. Za podatke v realnem času smo uporabili varne API klice z avtentikacijskimi žetoni, ki so bili vključeni v glave zahtev. Ko uporabnik zahteva te podatke se avtenticirani zahtevki preko OPSI konektorja posredujejo do MOC konektorja, ki nato pridobi najnovejše podatke iz sistemov MOC. Ta način omogoča MOC nadzor nad tem, kdo lahko dostopa do določenih kategorij podatkov. Za testiranje in odpravljanje napak REST API klicev se je uporabilo orodje Postman.

Varnost sistema se je zagotovilo z integracijo DAPS (Dynamic Attribute Provisioning Service) za dinamično preverjanje atributov in implementacijo sistemov za upravljanje z digitalnimi certifikati. Za uporabniški del sistema je bila razvita nadzorna plošča MOC in uporabniški vmesnik OPSI z uporabo ogrodja Angular, pri čemer je bila posebna pozornost namenjena funkcionalnostim za pridobivanje podatkov in njihovo vizualizacijo. V našem primeru smo razvili interaktivni prikaz, kjer je za vsako parkirišče MOC označen odstotek zasedenosti. Ob izbiri posameznega parkirišča se uporabniku prikaže zemljevid z natančno lokacijo, kar omogoča hitro načrtovanje poti.

Zadnja faza implementacije je vključevala obsežno testiranje in optimizacijo. Razvili so se testi za preverjanje delovanja posameznih komponent ter testi za preverjanje integracije celotnega sistema.

4.4.2 Izzivi in rešitve

Med implementacijo smo se soočili s številnimi izzivi. Eden glavnih je bila kompleksnost IDS protokolov, ki smo jo premagali z intenzivnim študiranjem dokumentacije in pogostimi sestanki. Integracija z obstoječim sistemom MOC je predstavljala dodaten izziv, ki smo ga rešili z razvojem prilagojenih API klicev in implementacijo vmesne programske opreme.

Zagotavljanje konsistentnosti podatkov je zahtevalo implementacijo naprednih mehanizmov za sinhronizacijo in preverjanje integritete podatkov. Soočili smo se tudi z izzivom učenja novih tehnologij, zlasti ogrodja Angular.

4.4.3 Uporabljena orodja in tehnologije

Pri razvoju sistema se je uporabilo vrsto orodij in tehnologij. IDS Testbed je služil za simulacijo MVDS, medtem ko je bil za kontejnerizacijo komponent uporabljen Docker. Konfiguracija in avtomatizacija konektorjev je bila izvedena preko Python skript, izgled uporabniških vmesnikov pa realiziran z uporabo ogrodja Angular. Komunikacija med komponentami se je omogočila preko REST API-jev, za upravljanje z varnostnimi atributi pa smo implementirali DAPS. Za verzioniranje kode smo uporabljali Git, kar nam je omogočilo učinkovito sodelovanje in sledenje spremembam.

Slika 3: **Uporabniški vmesnik na OPSI**

4.4.4 Arhitektura sistema

Arhitektura našega sistema temelji na komponentah, ki so prikazane na sliki 4. MOC konektor služi kot vmesnik med sistemom in MOC podatkovnim jezerom ter context brokerjem. OPSI konektor omogoča dostop do podatkov preko OPSI portala. DAPS skrbi za dinamično preverjanje atributov in tako zagotavlja varnost sistema. Nadzorna plošča MOC, razvita kot Angular aplikacija, prikazana na sliki 2, omogoča učinkovito upravljanje s podatki. Uporabniški vmesnik OPSI, ki je prav tako razvit v Angularju in je razviden na sliki 3, pa služi za prikaz podatkov končnim uporabnikom.

4.4.5 Rezultati

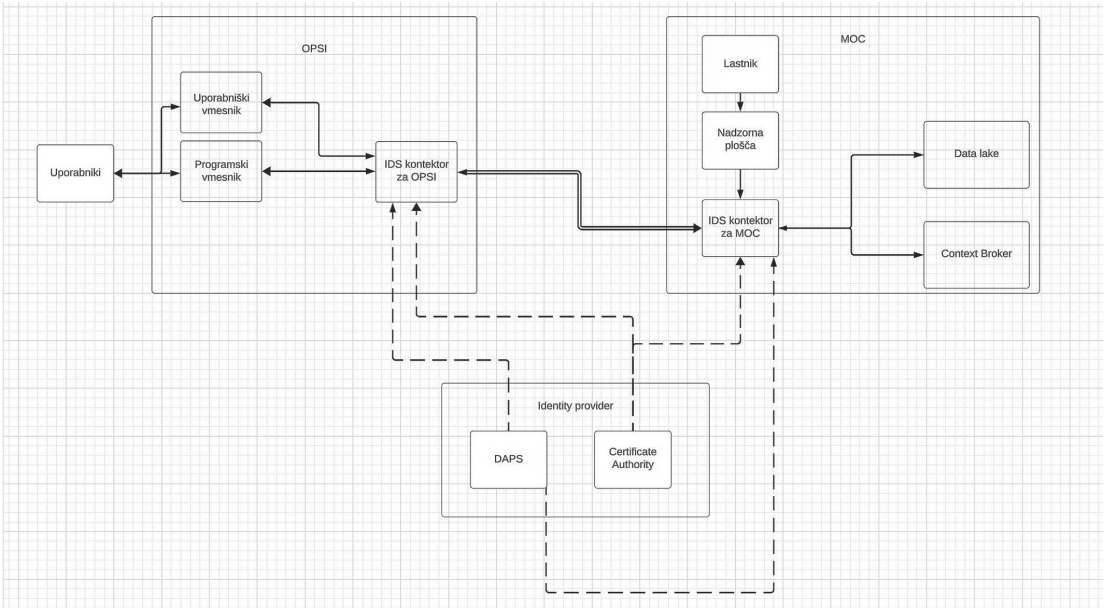
Naš sistem uspešno omogoča:

- Varno in nadzorovano izmenjavo podatkov med MOC in OPSI
- Enostaven pregled in vizualizacijo podatkov o zasedenosti parkirišč za končne uporabnike
- Fleksibilno upravljanje s podatkovnimi zbirkami in pravicami dostopa za skrbnike MOC
- Decentralizirano shranjevanje podatkov v skladu z načeli podatkovne suverenosti

Ta implementacija predstavlja korak naprej v smeri standardizirane in varne izmenjave podatkov med javnimi institucijami in lahko služi kot vzorčni primer za podobne projekte v drugih občinah ali organizacijah.

5 ZAKLJUČEK

Podatkovni prostori predstavljajo pomemben korak naprej v smeri varne in standardizirane izmenjave podatkov, ki prinaša številne prednosti za različne sektorje, vključno z javno upravo. Implementacija podatkovnega prostora med Mestno občino Celje in portalom Odprti Podatki Slovenije je pokazala, kako lahko podatkovni prostori izboljšajo upravljanje in deljenje podatkov, povečajo varnost ter omogočijo boljšo interoperabilnost med različnimi entitetami. Ključni elementi, kot so IDS standardi, decentralizirano shranjevanje podatkov in napredne varnostne rešitve, omogočajo zaupanje med partnerji in varno deljenje podatkov.



Slika 4: **Arhitektura sistema**

V prihodnosti bo ključnega pomena nadaljnji razvoj in širjenje podatkovnih prostorov, ki bodo podpirali digitalno preobrazbo in gospodarsko rast. Uporaba podatkovnih prostorov v javni upravi, kot je prikazano na primeru Mestne občine Celje, lahko služi kot model za druge občine in organizacije, ki si prizadevajo za izboljšanje svojih storitev in učinkovitejše upravljanje virov.

Standardizacija in interoperabilnost podatkov ostajata temeljna izziva, ki ju je potrebno naslavljati z nadaljnjim razvojem tehnologij in vzpostavitvijo jasnih regulativnih okvirov. Le tako bomo lahko v celoti izkoristili potencial podatkovnih prostorov in prispevali k bolj povezani, inovativni in varni podatkovno usmerjeni družbi.

Prizadevanja za nadaljnjo širitev podatkovnih prostorov bodo ključna za spodbujanje inovacij in gospodarske rasti. S sodelovanjem med javnimi institucijami, podjetji in raziskovalci lahko ustvarimo robustne podatkovne ekosisteme, ki bodo podpirali trajnostni razvoj in izboljšali kakovost življenja za vse državljane.

6 ZAHVALA

Radi bi se zahvalili izr. prof. dr. Dejanu Lavbiču za idejo, pobudo in mentorstvo pri projektu. Prav tako se zahvaljujemo viš. pred. dr. Aljažu Zrnecu in asist. dr. Marku Poženelu za njuno strokovno mentorstvo. Zahvala gre tudi Mestni občini Celje za zagotavljanje podatkov, ki so omogočili izvedbo projekta.

7 LITERATURA

[1] European Commission. »European Data Strategy.« Accessed: 2024-07-10. (2020), spletni naslov: https://commission.europa.eu/strategy- and- policy/priorities- 2019- 2024/europe- fit- digital-age/european-data-strategy_en.

[2] European Commission. »Data Governance Act.« Accessed: 2024-07-10. (2023), spletni naslov: https: //digital-strategy.ec.europa.eu/en/policies/data-governance--act.

[3] European Commission. »Data Spaces.« Accessed: 2024-07-10. (2023), spletni naslov: https :// joinup.ec.europa.eu/collection/semic-support-centre/data-spaces.

[4] Gaia-X. »About Gaia-X.« Accessed: 2024-07-10. (2023), spletni naslov: https://gaia-x.eu/what- is-gaia-x/about-gaia-x/.

[5] International Data Spaces Association. »Goals of the International Data Spaces.« Accessed: 2024-07-10. (2023), spletni naslov: https://docs.internationaldataspaces.org/ids-knowledgebase/v/ ids-ram-4/introduction/1_1_goals_of_the_international_data_spaces.

[6] International Data Spaces Association (IDSA). »Dataspace Connector.« Accessed: 2024-07-18. (2024), spletni naslov: https : / / international - data - spaces - association . github . io / DataspaceConnector/.

[7] International Data Spaces Association (IDSA). »International Data Spaces.« Accessed: 2024-07-18. (2024), spletni naslov: https://internationaldataspaces.org/.

[8] Odprti podatki Slovenije. »O portalu.« Accessed: 2024-07-3. (2023), spletni naslov: https://podatki. gov.si/o-portalu.

[9] B. Otto, »The evolution of data spaces,« v Designing data spaces: The ecosystem approach to competitive advantage, Springer International Publishing Cham, 2022, str. 3–15.

[10] Urad za publikacije Evropske unije, European data spaces and the role of data.europa.eu. Urad za publikacije Evropske unije, 2023, str. 15. DOI: doi/10.2830/1603.

▪

Ruben Ferreira je dodiplomski študent drugega letnika računalništva in informatike na Univerzi v Ljubljani. Kot član ekipe IDealni Scenarij je z rešitvijo o podatkovnih prostorih osvojil prvo mesto na Arnesovem hekatonu.

▪

Erazem Stanonik je dodiplomski študent tretjega letnika računalništva in informatike na Univerzi v Ljubljani. Kot član ekipe IDealni Scenarij je z rešitvijo o podatkovnih prostorih osvojil prvo mesto na Arnesovem hekatonu.

▪

Jana Volk je dodiplomska študentka tretjega letnika računalništva in informatike na Univerzi v Ljubljani. Kot članica ekipe IDealni Scenarij je z rešitvijo o podatkovnih prostorih osvojila prvo mesto na Arnesovem hekatonu.

▪

Alen Cigler je dodiplomski študent tretjega letnika računalništva in informatike na Univerzi v Ljubljani. Kot član ekipe IDealni Scenarij je z rešitvijo o podatkovnih prostorih osvojil prvo mesto na Arnesovem hekatonu.

▪

Hana Skitek je dodiplomska študentka tretjega letnika računalništva in informatike na Univerzi v Ljubljani. Kot članica ekipe IDealni Scenarij je z rešitvijo o podatkovnih prostorih osvojila prvo mesto na Arnesovem hekatonu.

Kibernetski napadi preko stranskih kanalov

Tjaž Štok, Matevž Pesek
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Večna pot 113, 1000 Ljubljana
ts92284@student.uni-lj.si, matevz.pesek@fri.uni-lj.si

Izvleček

Pri implementaciji kriptografskih operacij v programskih rešitvah pogosto posegamo po optimizaciji programske kode z namenom zmanjšanja dodatnega časa, potrebnega za izračun. Takšne odločitve imajo lahko negativne posledice na uhajanje podatkov izven programske rešitve. Napadalci lahko izkoristijo dodatne informacije, ki nastajajo pri izvedbi programske rešitve, na način, ki jim omogoča dodatne vpoglede v delovanje programa, izračunane vrednosti in dostop do samih podatkov. Vpoglede lahko pridobivajo v obliki časa izvedbe, vzorca dostopa do pomnilnika, porabe energije in drugih, na videz nepovezanih parametrov sistema. Takšne napade imenujemo »napadi preko stranskih kanalov«.

Članek predstavlja več primerov takšnih napadov in razsežnosti uhajanja informacij ter načinov zaščite pred napadi. Opisane so časovna kriptoanaliza, kriptoanaliza na podlagi porabe energije in njena posebna različica – kriptoanaliza na podlagi videoposnetka – ter pomnilniška kriptoanaliza. Na primeru preprostega napada s časovno kriptoanalizo je predstavljen postopek analize in rezultati pred in po implementaciji predlagane zaščite.

Ključne besede: kibernetska varnost, kriptoanaliza, kriptografija, napadi preko stranskih kanalov

Exploiting side-channel attacks in cybersecurity

Abstract

When implementing cryptographic primitives in software, we often resort to optimizing the software code in order to reduce unnecessary computation time. Such decisions can have negative consequences on data leakage outside the implementation. Attackers can exploit the additional information generated by the execution of the software solution in a way that gives them additional insights into the operation of the software, the values calculated and access to the data itself. Insights can be gained in the form of execution time, memory access patterns, power consumption, and other seemingly unrelated system parameters. Such attacks are referred to as »side-channel attacks«.

This paper presents several examples of such attacks and the magnitude of information leakage, as well as how to protect against such attacks. Time-based cryptanalysis, power-based cryptanalysis, including a special variant – video-based cryptanalysis – and memory-based cryptanalysis are described. A simple timing cryptanalysis attack is used as an example to present the analysis process and the results before and after the implementation of the proposed mitigation.

Keywords: cybersecurity, cryptanalysis, cryptography, side-channel attacks

1 UVOD

Kriptografija dandanes postaja vse bolj pomembna stroka, saj digitalni podatki predstavljajo vse od zasebnosti individualne osebe do strogo tajnih državnih skrivnosti. Skozi zadnja desetletja so bili razviti in preizkušeni različni načini zagotavljanja digitalne tajnosti, ki jih v današnjem času uporabljamo že pri vsakdanjih opravilih, kot je opravljanje nakupov preko spleta, dostop do spletne banke in drugih. Kljub temu, da so današnji kriptografski sistemi prestali že veliko napadov in formalnih preverjanj, niso nujno popolnoma odporni na drugačno vrsto napadov: napadi preko stranskih kanalov (angl. *side-channel attacks*). Ti napadi izkoriščajo informacije iz drugih,

nepredvidenih virov (npr. [2]), kot so na primer merjenje časa, merjenje porabe energije, merjenje elektromagnetnega sevanja in drugih zunanjih dejavnikov delovanja sistema.

Namen tega članka je pregled različnih *side-channel* napadov, njihove pomembnosti, načinov izvedbe in možnosti za preprečevanje napadov. Po metodološkem pregledu napadov tega tipa sprva predstavimo časovno kriptoanalizo, ki prikazuje tveganja pri optimizaciji izvajanja ali implementaciji občutljivih kriptografskih operacij. Zatem predstavimo kriptoanalizo na podlagi porabe energije, s katero je poudarjena nezadostnost uporabe konstantno-časovnih algoritmov na modernih centralnih procesnih enotah, saj lahko z analizo porabe dejanske energije in spreminjanja period ure centralne procesne enote glede na porabo spremljamo uhajanje informacij. Nadalje predstavimo kriptoanalizo na podlagi videoposnetka, kjer analiziramo svetilnost LED diode, iz katere je mogoče inducirati porabo energije. Nazadnje na kratko omenimo pomnilniško kriptoanalizo, s katero je zaradi neprevidne implementacije optimizacije predpomnilnika mogoče izluščiti tajne kriptografske ključe iz predpomnilnika centralnih procesnih enot Apple M1.

2 METODOLOGIJA RAZISKOVALNEGA PRISTOPA NAČRTOVANJA IN RAZVOJA

V tej raziskavi smo uporabili raziskovalni pristop načrtovanja in razvoja (angl. *design science methodology* - DSM) za sistematično analizo in ublažitev napadov preko stranskih kanalov na implementacije kriptografskih programov. Proces smo pričeli s temeljito fazo identifikacije problema, pri čemer smo ugotovili, da optimizacija kriptografskega programa za zmanjšanje časa izračunavanja nenamerno uvaja ranljivosti. Te ranljivosti lahko izkoristimo za napade preko stranskih kanalov, kot so časovna kriptoanaliza, kriptoanaliza na osnovi porabe energije, video kriptoanaliza in kriptoanaliza na osnovi pomnilnika. Rezultat identifikacije v tej raziskavi je razviti praktične in učinkovite rešitve, ki ublažijo te vrste napadov, ne da bi pri tem spreminjali delovanja ali namena procesa.

V praktičnem delu članka je naš cilj ustvariti protiukrepe, ki bi učinkovito onemogočili uhajanje informacij skozi stranske kanale. Specifično smo si prizadevali razviti tehnike, ki ohranjajo koristi optimizacije programa, hkrati pa zmanjšujejo tveganje uhajanja informacij. Ukrepe smo načrtovali z namenom uporabe v realnih scenarijih in zagotavljanju robustnih implementacij kriptografskih operacij.

Med fazo načrtovanja in razvoja smo oblikovali različne strategije za ublažitev različnih vrst stranskih napadov. Za časovno kriptoanalizo smo zasnovali algoritme s konstantnim časom in preprečili variacije v času trajanja glede na vhodne podatke, da bi zameglili časovne vzorce. Kriptoanalizo na osnovi porabe energije smo obravnavali z izvajanjem tehnik uravnoteženja porabe energije. Za preprečevanje video kriptoanalize smo poleg nasvetov za preprečevanje kriptoanalize na podlagi porabe energije tudi predlagali ločeno električno vezje za statusne LED diode. Za kriptoanalizo na osnovi pomnilnika smo zagotovili konstantne vzorce dostopa do pomnilnika. Vsaka od teh strategij je bila zasnovana za obravnavo specifičnih značilnosti in ranljivosti, povezanih z ustreznimi vektorji stranskih napadov. Praktičnost in učinkovitost teh rešitev prikazujemo s študijami primerov.

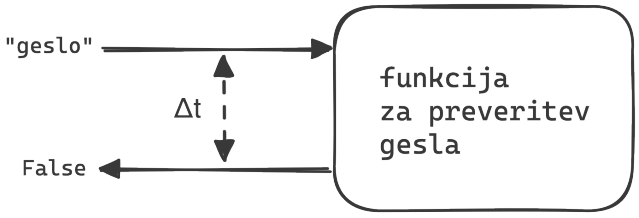
3 PREGLED PODROČJA

Nevarnosti časovne kriptoanalize so sprva demonstrirali Kocher in drugi [4], ki so uspešno pridobili faktorizacijo RSA ključev in Diffie-Hellman eksponente, ta napad pa so kasneje dodelali Dhem in drugi [2] s praktičnim napadom na sistem bralnikov varnostnih kartic. Dovzetnost na časovno kriptoanalizo izhaja iz dolgoletnega truda za boljšo optimizacijo strojne kode, ki jo ustvarijo programski prevajalniki. To je privedlo do razvoja principa izvedbe v konstantnem času, ki zagotavlja, da se kriptografske operacije vedno končajo v približno enakem času ne glede na veljavnost vhodnega podatka [6].

Časovna kriptoanaliza je bila iztočnica za razvoj novih vrst napadov, kot so analiza porabe energije [3][8], ki lahko zaradi narave računalnikov in optimizacije delovanja centralne procesne enote razkrije veliko o stanju kriptografskega sistema. Poleg vpogleda v porabo energije lahko veliko razkrije tudi dostop do (pred)pomnilnika, kar so demonstrirali Vicarte in drugi [7] z napadom *Augury* ter Chen in drugi [1] z napadom *GoFetch*. Razviti so bili tudi bolj eksotični napadi, kot je neinvazivna videoanaliza LED diode bralnika varnostnih kartic [5], ki je omogočila pridobitev tajnega kriptografskega ključa kartic iz bralnika.

3.1 Časovna kriptoanaliza

Časovna kriptoanaliza temelji na statistični analizi časa izvedbe kriptografskih operacij, iz katere lahko ugotovimo njihov notranji mehanizem in v nekaterih primerih celo postopoma sestavimo tajni kriptografski ključ ali geslo. Slika 1 ilustrira abstrakten model tega tipa napada.



Slika 1: **Princip merjenja časa kriptografske funkcije.**

V najpreprostejšem primeru gre za funkcijo, ki preveri, ali je podano geslo pravilno tako, da preveri ujemanje vsakega bajta v pravilnem (shranjenem) geslu. Če naleti na neujemanje bajtov, se funkcija takoj zaključi in vrne rezultat *False*, četudi ni preverila vseh bajtov, saj eno neujemanje že predstavlja napačno geslo. Optimizacija predstavlja tveganje, saj lahko napadalec glede na čas, ki ga funkcija porabi, ugotovi, ali je določen znak pravilen. Če napadalec odkrije ujemanje prvega bajta, lahko opazi, da je funkcija za preverjanje trajala dlje kot prej, saj se je lotila preverjanja naslednjega bajta. Tako lahko napadalec postopoma zgradi geslo zgolj s pomočjo merjenja časa. Algoritem za naivno preverjanje gesla je predstavljen s psevdokodo v Algoritmu 1.

Algoritem 1 Psevdofunkcija za naivno preverbo gesla.

```
1: function check_password(input)
2:     password ← "password"
3:     if |input| ≠ |password| then
4:         return False
5:     for ∀i ∈ {0,1,...,|password|−1} do
6:         if input[i] ≠ password[i] then
7:             return False
8:     return True
```

Preprost, vendar zelo efektiven način ublažitve opisanega napada je izogibanje zgodnjemu vračanju iz funkcije, kadar pride do neujemanja. Če torej pride do neujemanja bajtov v vhodnem geslu, vseeno pustimo da se zanka zaključi in šele nato vrnemo rezultat *False*. Temu konceptu pravimo izvedba v konstantnem času (angl. *constant-time programming*), saj čas izvedbe ni odvisen od vhodnega podatka. Izboljšan algoritem je prikazan v Algoritmu 2 s predpostavko, da je vhodno geslo enake dolžine kot pravilno. V nasprotnem primeru lahko z namenom upoštevanja principa programiranja v konstantnem času preostali prostor zapolnimo s praznimi (*NULL*) znaki.

Algoritem 2 Psevdofunkcija za preverbo gesla v konstantnem času.

```
1: function check_password_constant_time(input)
2:     password ← "password"
3:     result ← |input| = |password|
4:     for ∀i ∈ {0,1,...,|password|−1} do
5:         state ← state ∧ (input[i] = password[i])
6:     return state
```

Alternativno rešitev bi lahko predstavljala tudi zgoščevalna funkcija, ki bi jo uporabili za primerjavo zgoščenih vrednosti pravilnega gesla in vhodnega podatka. Dokler je zgoščevalna funkcija implementirana po principu programiranja v konstantnem času, je časovna analiza primerjave bajtov gesel praktično neuporabna, saj izhodna vrednost kriptografske zgoščevalne funkcije ne poda informacije o vhodni vrednosti.

Morebitnega napadalca lahko upočasni tudi omejevanje števila klicev funkcije v določeni časovni enoti, vendar se je potrebno zavedati, da to ni popolna rešitev in je le dodatek k izvedbi v konstantnem času.

Pri pisanju kriptografskih funkcij je potrebno pozornost usmeriti tudi k programskim prevajalnikom. Slednji lahko namreč nenamerno optimizirajo kodo in s tem prekršijo princip izvajanja v konstantnem času. Prevajalniki so zelo kompleksni programi, ki tudi poskušajo optimizirati kodo zato, da odstranijo potratne ali neuporabljene ukaze, potratno rabo spomina in druge neuporabne operacije. Tak mehanizem optimizacije je marsikdaj (in večinoma) zaželen, vendar lahko v okviru kriptografije povzroči nezanemarljivo škodo. Med prevajanjem programa lahko prevajalnik odstrani namerne poti funkcij ali polnjenje spomina z ničlami (brisanje skrivnih vrednosti), zato so v sistemih in knjižnicah na voljo različni načini preprečevanja prevajalniških optimizacij.

Če želimo kriptografijo uporabiti v praksi, je zelo priporočljiva uporaba preizkušenih in formalno preverjenih knjižnic, saj se s tem lahko izognemo ponavljanju istih napak [6]. Pomembno je tudi temeljito preučiti in preizkusiti vsak del sistema ali programa, saj vsaka nenamerno izdana informacija iz varnega predela naprave (čas poteka, poraba energije, elek-

tromagnetno sevanje in drugi) predstavlja tveganje za napad preko stranskih kanalov.

3.2 Kriptoanaliza na podlagi porabe energije

Alternativni stranski kanal za napad je analiza porabe energije naprave, ki opravlja kriptografske operacije. Leta 1998 jo je demonstriral Kocher [3], ki je s pomočjo diferencialne analize sestavil DES enkripcijske ključe iz bralnikov kartic. Predstavljene so bile tudi rešitve, kot je konstantno-časovna izvedba in vpletanje šuma v energijsko analizo.

Soroden, vendar bolj sofisticiran napad *Hertzbleed* [8] temelji na merjenju porabe energije centralne procesne enote, ki mu sledi izvedba časovne kriptoanalize. Napad je izveden brez fizičnih merilnikov porabe električne energije, saj čas meri s pomočjo vmesnika za merjenje porabe energije v centralni procesni enoti. Pri tem napadu je močno izkoriščen koncept »*dinamično skaliranje frekvence in električne napetosti*« (angl. DVFS; *dynamic voltage and frequency scaling*). DVFS je ključen pri regulaciji temperature in porabe električne energije centralne procesne enote, saj se pri neaktivnosti procesorja frekvenca in napetost znižata, kar zmanjša porabo električne energije. Pri aktivni uporabi procesorja se frekvenca in električna napetost zvišata in tako omogočita hitrejše delovanje centralne procesne enote, znižata pa se pri visoki temperaturi ali električni moči nad določeno mejo z namenom preprečevanja pregrevanja čipov. Ker sta frekvenca in električna napetost odvisna od količine in načinov obdelovanja podatkov, pomeni, da je tudi frekvenca centralne procesne enote odvisna od teh podatkov. Obenem spremenjena frekvenca procesorske ure povzroči drugačen čas izvajanja, kar predstavlja možnost tudi za napad s časovno kriptoanalizo.

Za napad niso potrebni nobeni fizični instrumenti za merjenje porabe energije, kar pomeni, da je napad izvedljiv tudi na daljavo, vendar pod pogojem, da ima napadalec dostop do programskih vmesnikov za merjenje porabe energije in nivo električne napetosti na centralni procesni enoti. Ker je procesorska frekvenca odvisna od aktivnih operacij, so kriptografske operacije s principom izvedbe v konstantnem času dovzetne za napade s časovno kriptoanalizo, saj se glede na podan vhod kriptografski funkciji lahko spremeni procesorska frekvenca (in s tem čas izvedbe).

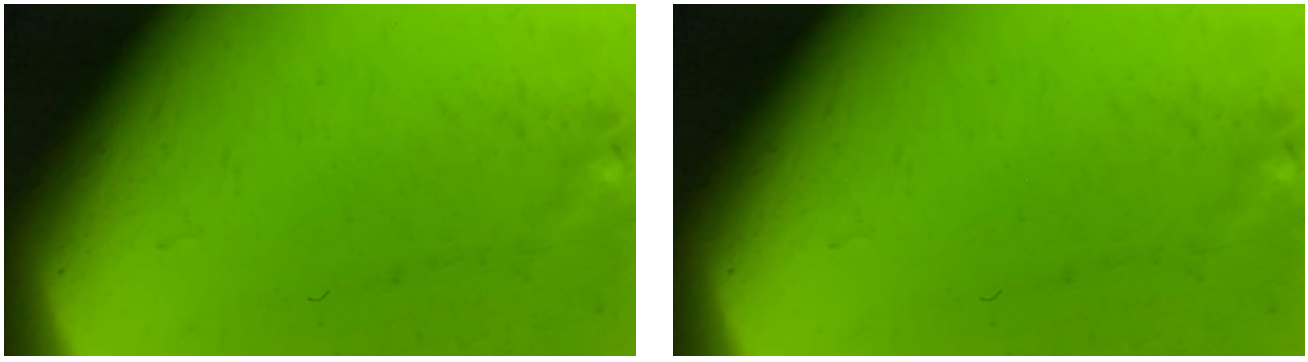
Najpreprostejša ublažitev takega napada je preprečevanje dostopa do vmesnikov za analizo procesorske frekvence in nivoja električne napetosti. Napadalec, ki želi izvesti kriptoanalizo na podlagi porabe energije, bo tako primoran v izvedbo fizičnega merjenja energije, kar je manj natančno in težje izvedljivo. Na področju opisanih napadov so ranljivi vsi moderni Intelovi in AMD-jevi procesorji, vendar obe podjetji priporočata naj avtorji kriptografskih knjižnic sami implementirajo programske popravke glede na izdane smernice.

Ugotovili smo, da so sprejete prakse izvedbe v konstantnem času pomanjkljive in jih je potrebno dodelati, saj lahko procesorji z dinamičnim spreminjanjem frekvence glede na vhodne podatke spremenijo čas izvedbe kriptografskih funkcij, ne glede na to, ali upoštevajo princip programiranja v konstantnem času.

3.3 Kriptoanaliza na podlagi videoposnetka

Tesno povezana s kriptoanalizo na podlagi porabe energije, kriptoanaliza na podlagi videoposnetka napadalcu omogoča izvedbo napada na naprave, ki uporabljajo statusno LED diodo za ponazarjanje delovanja naprave (npr. bralnik brezstičnih varnostnih kartic). Ko taki napravi približamo kartico, naprava prebere tajni kriptografski ključ, s pomočjo katerega opravi kriptografsko operacijo za preverbo veljavnosti kartice. Kadar bralnik sproži kriptografske operacije, se poraba električne energije na krmilniku zviša, zaradi česar se nivo energije na LED diodi zmanjša. Tako majhnih sprememb svetilnosti sicer ne moremo zaznati z golim očesom, lahko pa si pomagamo z video kamerami.

Pri tovrstnem napadu je uporabljena tehnika *rolling shutter*, ki omogoča, da namesto celega okvirja zajamemo več manjših odsekov (vertikalnih vrstic) vsake sličice videa, kar ustvari okoli 60,000 vzorcev na sekundo. Na ta način lahko z veliko višjo frekvenco analiziramo spremembe svetilnosti LED diode, razliko pa je mogoče zaznati s primerjavo sprememb barvnih vrednosti v RGB barvnem prostoru. S pomočjo teh vrednosti lahko induciramo, kakšna je bila sprememba nivoja energije na diodi in s tem zvišanje porabe energije na mikrokrmilniku. Vpogled v te podatke omogoča izvedbo napada na podlagi analize porabe energije (dokazano z napadom *Hertzbleed* [8]) in s tem pridobitev tajnih kriptografskih ključev na varnostnih karticah (npr. 256-bitni ECDSA tajni ključ).



Slika 2: **Razlika v svetilnosti/barvi LED diode med kriptografsko operacijo, ki je nevidna prostemu očesu. Povzeto iz [5] po licenci CC BY-NC.**

V primeru da ima naprava LED diodo vezano ločeno od mikrokrmilnika, je napad mogoč le pod pogojem, da ga preko USB razdelilca priklopimo na drugo napravo, ki ima LED diodo vezano vzporedno z mikrokrmilnikom [5]. Poleg uporabe pametnega telefona je napad izvedljiv tudi s pomočjo IP varnostnih kamer, ki se nahajajo v prostoru, kjer je nameščen bralnik. S predpostavko, da ima napadalec dostop do teh kamer, je napad izvedljiv tudi do 16 metrov razdalje med kamero in bralnikom varnostnih kartic. Postavitev, ki je bila potrebna za napad, je prikazana na Sliki 3.

Slika 3: **Postavitev, namenjena vzorčenju LED diode bralnika varnostnih kartic na oddaljenosti 16 metrov. Povzeto iz [5] po licenci CC BY-NC.**

Ranljivost sistema lahko proizvajalci omejijo tako, da ločijo vezji mikrokrmilnika in LED diode ali pa vzporedno vežejo kondenzator, ki gladi električno napetost, vendar takšne spremembe vodijo v višje cene produktov. Opomniti velja, da pomanjkljivosti ne ležijo v sami LED diodi, ampak v kriptografskih knjižnicah, ki neenotno porabljajo energijo, kar je v opisanem napadu izkoriščeno za analizo in pridobivanje tajnih kriptografskih ključev.

3.4 Pomnilniška kriptoanaliza

Nenehna optimizacija pomnilnikov in predpomnilnikov lahko poleg izboljšav vodi tudi v napake, ki povečujejo ranljivost za napade. Ena izmed najnovejših ponesrečenih optimizacij je bila Applova implementacija tako imenovanega DMP-ja (angl. *Data Memory-Dependent Prefetcher*), ki je iteracijo po tabeli pomnilniških kazalcev pospešil tako, da je v predpomnilnik naložil več podatkov naenkrat. Poleg tega je

vsako vrednost v predpomnilniku, ki je »izgledala« kot kazalec, samodejno naložil [7].

Pri tem procesu problem predstavlja kršitev principa konstantne izvedbe operacij, saj lahko nepredvideno posega po pomnilniku.

Ranljivost je sprva demonstriral napad *Augury* [7], kasneje pa je bila z napadom *GoFetch* [1] izpostavljena še ranljivost tajnih kriptografskih ključev. S tem napadom je kriptoanalizo mogoče izvesti tudi na kriptografskih funkcijah, ki delujejo v konstantnem času.[1]

Za preprečevanje opisanega napada obstajajo trije različni pristopi:

1. **Uporaba »učinkovitih jeder«:** Applovi M1 procesorji so razdeljeni na dve gruči – »učinkovita jedra« (angl. *Efficiency Cores*) in »visokozmogljiva jedra« (angl. *High-Performance Cores*), pri čemer učinkovita jedra nimajo aktiviranega DMP-ja. Izvajanje kriptografskih funkcij bi lahko omejili na ta jedra, vendar bi se zmogljivost pri izvedbi kriptografskih operacij zmanjšala, saj bi se izvajale počasneje. Poleg počasnejšega delovanja bi tvegali tudi morebitne težave zaradi potencialne odločitve proizvajalca za aktivacijo DMP-ja tudi na učinkovitih jedrih.
2. **Slepljenje:** Razvijalci kriptografskih knjižnic bi lahko implementirali princip *»slepljenja«*, ki maskira prave vrednosti kriptografskih skrivnosti, preden so zapisane v pomnilnik. Negativna plat tega pristopa je, da v kriptografske knjižnice prinaša povišano kompleksnost in upočasnitev.
3. **Onemogočanje DMP-ja za nekatere operacije:** Proizvajalec bi lahko omogočil možnost, da razvijalci kriptografskih knjižnic eksplicitno onemogočijo DMP pri opravljanju kriptografskih operacij.

4. PREDSTAVITEV PRIMERA

Med raziskavo smo opravili statistično analizo preproste časovne kriptoanalize, s katero poudarjamo nevarnost takih napadov. Napad smo izpeljali v dveh fazah: v prvi smo poskusili uganiti dolžino gesla, v drugi pa posamezne znake v geslu. Struktura programa je sledeča:

- Funkcija za merjenje časa: S pomočjo Python knjižnice *timeit* merimo čas izvajanja n ponovitev določene funkcije z določenimi argumenti in vrnemo seznam k časov. Iz tega seznama vzamemo najmanjšo vrednost, ki predstavlja lokalno najboljši čas. Funkcija izbrani čas izvajanja določene funkcije izpiše v mikrosekundah.
- Funkcija za ugibanje dolžine gesla: Funkcija izbere diskretni interval, ki predstavlja potencialne dolžine gesla (v našem primeru od 1 do 15 znakov) ter primerja čas izvajanja naključnih gesel (v našem programu smo izbrali nize zapolnjene z n ponovitvami znaka A), pri čemer je niz ob vsaki ponovitvi daljši za en znak (do konca izbranega intervala). Po koncu vzorčenja funkcija izbere geslo, za katerega je funkcija porabila najdlje, s predpostavko, da funkcija za preverjanje gesel takoj zavrne gesla napačne dolžine in preverja le znake vnosov pravilnih dolžin. Funkcija vrne dolžino gesla z najvišjo verjetnostjo pravilnosti.
- Funkcija za ugibanje gesla: Funkcija kot vhod sprejme dolžino gesla, ki smo ga v našem primeru določili s funkcijo za ugibanje dolžine gesla. Pred izbiro znakov je ustvarjen seznam vseh znakov, ki jih lahko sprejme funkcija za preverjanje (v našem primeru male tiskane črke angleške abecede), nato pa v vsaki iteraciji zanke dodamo nov znak na konec gesla, ki ga gradimo. Pri tem merimo čas, ki je porabljen za vsak znak na koncu trenutno zgrajenega gesla (da je preizkusno geslo pravilne dolžine, mu na konec dodamo naključne znake). Kot »pravilen« znak sprejmemo tistega, za katerega je funkcija za preverjanje gesla porabila največ časa, saj sklepamo, da je znak pravilen in se je funkcija za preveritev gesla premaknila na naslednji znak. Ko dosežemo zahtevano dolžino gesla, lahko sklepamo, da smo sestavili geslo, ki je zelo podobno (ali enako) pravilnemu geslu pod pogojem, da smo glede na dolžino gesla izbrali dovolj visoko število vzorcev pri merjenju časa.

[1] Napad je bil uspešno izveden na *OpenSSL*-ovi implementaciji tradicionalne *Diffie-Hellman* izmenjave ključev, Gojeve implementacije RSA dešifriranja *CRYSTALS-Kyber* in *Crystals-Dilithium*.

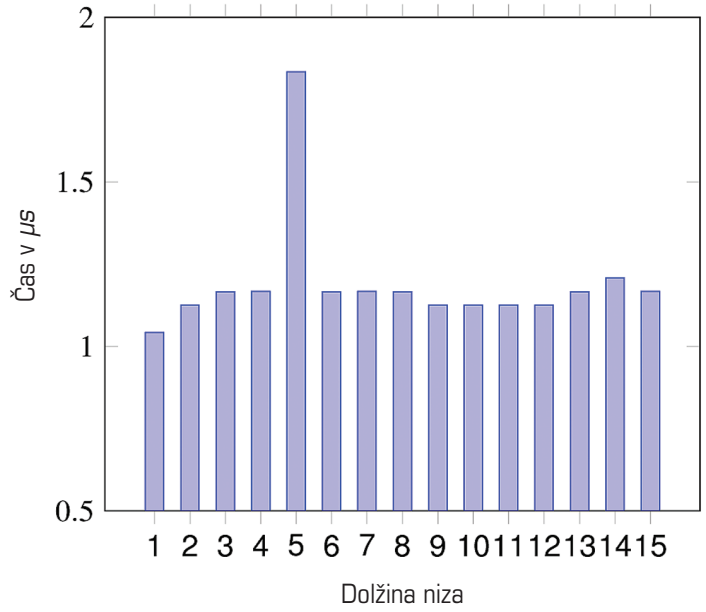
Za tarčo napada smo izbrali Python implementacijo Algoritma 1, ki je prikazana v izvorni kodi 1.

```python
def check_password (input_password: str):

    correct_password = "geslo".encode("utf-8")
    input_password = input_password.encode("utf-8")

    if len(input_password) ≠ len(correct_password):
        return False

    for i in range(len(correct_password)):
        if input_password[i] ≠ correct_password[i]:
            return False

    return True
```

Izvorna koda 1: **Python koda, ki naivno preveri ujemanje gesel.**

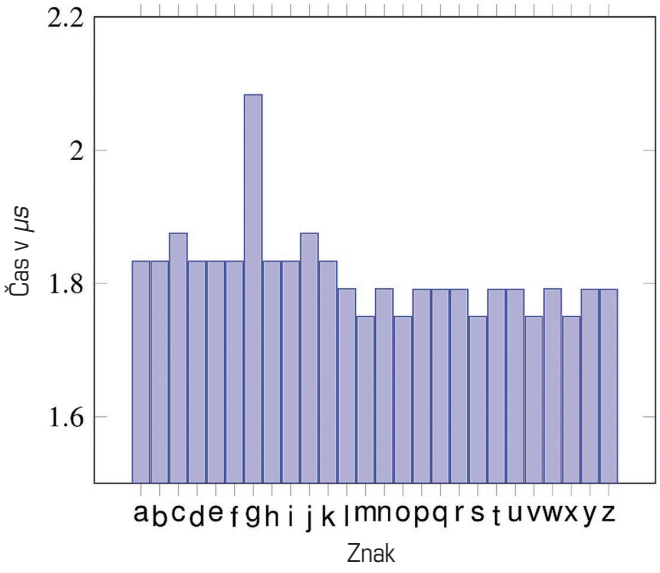
Iz poskusov smo ugotovili, da je za krajša gesla (do 10 znakov) zadovoljiva velikost vzorca $N = 100$, ko gre za poskus ene dolžine ali znaka, kar pomeni grupiranje 10 iteracij funkcije po 10 izvedb poskusov. Iz tega postopka izberemo najmanjšo časovno vrednost, zato da ovržemo odstopanja zaradi nepredvidenih sistemskih upočasnitev. Pri daljših geslih se je natančnost ugibanja nekoliko zmanjšala, vendar je za izboljšanje zadostoval povečan vzorec (do $N = 500$). Obe fazi podrobno analiziramo:

1. Izbrali smo interval dolžin gesla $L = \{1 \leq x \leq 15 | x \in \mathbb{Z}^{0+}\}$ in za vsako diskretno dolžino $l \in L$ preizkusili naključni niz simbolov te dolžine. Po vzorčenju smo s seznama časov izbrali dolžino niza, ki jo je funkcija procesirala najdlje (torej se je dolžina ujemala s pravim geslom in je program preveril ujemanje *vsaj* prvega bajta nizov). Iz Slike 4 je jasno razvidno, da je v našem primeru najverjetnejša dolžina pravega gesla 5.



Slika 4: **Rezultati vzorčenja dolžin naključnih nizov.**

2. Z izbrano dolžino $l \in L$ iz prejšnje faze smo nato pognali proces ugibanja vsakega znaka pravilnega gesla. Funkciji smo z vsako iteracijo posredovali trenutno potrjen niz in naključne znake, s katerimi je bila zapolnjena dolžina. Sprva smo izbrali nabor znakov in nato vsak znak iz množice vzorčili večkrat (npr. $N = 100$; isto kot pri vzorčenju dolžine, 10 zaporednih iteracij funkcije v 10 ločenih izvedbah). Pri tem smo beležili najkrajši čas, ki ga je porabila funkcija za vsak znak (za primerjavo najboljših primerov) in izmed vseh izbrali tistega, za katerega je funkcija porabila največ časa. Izbrani znak smo dodali na konec trenutnega niza in se premaknili na naslednjo iteracijo. To smo ponavljali dokler nismo dosegli dolžine niza, določene v predhodni fazi.



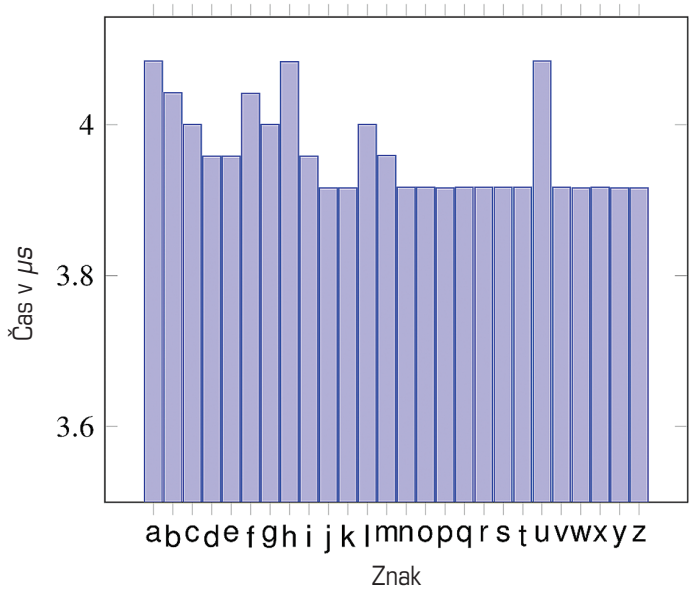
Slika 5: **Rezultati vzorčenja prvega znaka v geslu.**

Iz Slike 5 je razvidno, da je bil v našem primeru najverjetneje prvi znak gesla črka *g*. Ob koncu iteracij napada smo s pomočjo preproste statistične analize in naivno implementirane funkcije našli geslo »*geslo*«. Poskusili smo opraviti tudi časovni napad nad našo kriptografsko funkcijo, ki je izvedena v konstantnem času. Python implementacija funkcije je prikazana v izvorni kodi 2.

Ugotovili smo, da ni mogoče več zanesljivo predvideti, kateri znak je pravilen, saj so bili vsi izmerjeni časi trajanja funkcije zelo podobni in brez očitnega vzorca. Primerjava časovnega poteka funkcije s prvim znakom (s predpostavko, da poznamo dolžino pravilnega gesla) je predstavljena na Sliki 6.

```python
def check_password_constant_time (input_password: str):

    correct_password = "geslo".encode("utf-8")
    input_password = input_password.encode("utf-8")
    result = True

    for i in range(len(correct_password)):
        result &= len(input_password) > i and input_password[i] == correct_password[i]

    return result
```

Izvorna koda 2: **Python koda, ki preveri ujemanje gesel v konstantnem času.**



Slika 6: **Rezultati vzorčenja prvega znaka pri izvedbi v konstantnem času.**

5. DISKUSIJA IN ZAKLJUČEK

V članku smo predstavili različne vrste napadov preko stranskih kanalov, opisali smo njihove značilnosti in načine zaščite pred njimi. Ugotovili smo, da je razlog za njihov obstoj večinoma neprevidna implementacija kriptografskih operacij in agresivna optimizacija prevajalnikov.

Kot prvo smo predstavili časovno kriptoanalizo, utemeljeno na merjenju časa, ki ga porabi kriptografska funkcija. Napadalec lahko s preprostim statističnim modelom predvidi dolžino gesla in znake, ki najverjetneje tvorijo geslo. Kot drugo smo opisali kriptoanalizo na podlagi porabe energije, ki s pomočjo diferencialne analize stanja centralne procesne enote (sprememba električnega toka ali trenutna frekvenca procesorske ure in električna napetost) ter pošiljanja raznih tajnopisov kriptografski funkciji (tako imenovan napad z izbranim tajnopisom) omogoča napadalcu odkritje tajnega kriptografskega ključa. Predstavili smo tudi kriptoanalizo na podlagi videoposnetka, ki s pomočjo pametnega telefona ali IP kamere analizira LED diodo kriptografske naprave (npr. bralnika varnostnih kartic) in inducira porabo energije med izvajanjem kriptografskih operacij, kar omogoči kriptoanalizo na podlagi porabe energije.

Nazadnje smo predstavili tudi pomnilniško kriptoanalizo, s katero je zaradi neprevidne implementacije optimizacije predpomnilnika moč izluščiti tajne kriptografske ključe iz predpomnilnika Applovih centralnih procesnih enot serije M1.

Opravili smo tudi preprost prikaz napada s časovno kriptoanalizo, ki ilustrira pomembnost upoštevanja principov izvedbe v konstantnem času.

S člankom smo želeli izpostaviti dejstvo, da so stranski kanali zelo nepredvidljivi in lahko ogrožajo obstoječe kriptografske sisteme, na katere se vsakodnevno zanaša veliko število uporabnikov. Razumevanje teh napadov je ključnega pomena v kriptografiji, kadar želimo izpopolniti kriptografske funkcije in zmanjševati njihove šibkosti. Hkrati se je pomembno zavedati, da popolnost teoretičnih modelov težko zagotovi popolnoma odporne kriptografske funkcije v praksi, saj napadi preko stranskih kanalov izkoriščajo ranljivosti njihovih implementacij in sistemov, na katerih se le-te izvajajo.

V zadnjih letih se je kriptografija kot veda zelo razširila in dandanes vse več raziskovalcev namenja pozornost odkrivanju novih vrst napadov in zaščit pred njimi. Z večanjem kompleksnosti računalniških sistemov lahko pričakujemo, da bo v prihodnosti prihajalo do vse bolj kompleksnih napadov, ki bodo predstavljali nove izzive pri implementaciji kriptografskih funkcij.

LITERATURA

[1] Boru Chen, Yingchen Wang, Pradyumna Shome, Christopher W. Fletcher, David Kohlbrenner, Riccardo Paccagnella, and Daniel Genkin. Gofetch: Breaking constant-time cryptographic implementations using data memory-dependent prefetchers. In *USENIX Security*, 2024.

[2] Jean-François Dhem, François Koeune, Philippe-Alexandre Leroux, Patrick Mestré, Jean-Jacques Quisquater, and Jean-Louis Willems. A practical implementation of the timing attack. In Jean-Jacques Quisquater and Bruce Schneier, editors, *Smart Card Research and Applications*, pages 167–182, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.

[3] Paul Kocher, Joshua Jaffe, and Benjamin Jun. Differential power analysis. In Michael Wiener, editor, *Advances in Cryptology — CRYPTO' 99*, pages 388–397, Berlin, Heidelberg, 1999. Springer Berlin Heidelberg.

[4] Paul C. Kocher. Timing attacks on implementations of diffie-hellman, rsa, dss, and other systems. In Neal Koblitz, editor, *Advances in Cryptology — CRYPTO '96*, pages 104–113, Berlin, Heidelberg, 1996. Springer Berlin Heidelberg.

[5] B. Nassi, E. Iluz, O. Cohen, O. Vayner, D. Nassi, B. Zadov, and Y. Elovici. Video-based cryptanalysis: Extracting cryptographic keys from video footage of a device's power led captured by standard video cameras. In *2024 IEEE Symposium on Security and Privacy (SP)*, pages 166–166, Los Alamitos, CA, USA, may 2024. IEEE Computer Society.

[6] A. P. Shivarpatna Venkatesh, A. Bhat Handadi, and M. Mory. Security implications of compiler optimizations on cryptography – a review, 2019.

[7] Jose Rodrigo Sanchez Vicarte, Michael Flanders, Riccardo Paccagnella, Grant Garrett-Grossman, Adam Morrison, Christopher W. Fletcher, and David Kohlbrenner. Augury: Using data memory-dependent prefetchers to leak data at rest. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 1491– 1505, 2022.

[8] Yingchen Wang, Riccardo Paccagnella, Elizabeth Tang He, Hovav Shacham, Christopher W. Fletcher, and David Kohlbrenner. Hertzbleed: Turning power Side-Channel attacks into remote timing attacks on x86. In *31st USENIX Security Symposium (USENIX Security 22)*, pages 679–697, Boston, MA, August 2022. USENIX Association.

▪

Tjaž Štok je študent na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Zanimajo ga področja razvoja programske opreme in kibernetske varnosti. Njegovi raziskovalni interesi zajemajo teorijo kriptografije in razvoja varne programske opreme.

▪

Matevž Pesek je docent in raziskovalec na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, kjer je diplomiral (2012) in doktoriral (2018). Od leta 2009 je član Laboratorija za računalniško grafiko in multimedije. Od leta 2024 izvaja predmet Varnost programov.

Iz Islovarja

Islovar je spletni terminološki slovar informatike, ki ga od leta 2001 objavlja Slovensko društvo INFORMATIKA na naslovu http://www.islovar.org. Navajamo nekaj izrazov z slovarja:

copyleft -a [kópileft] m *(angl. copyleft)*
politika licenciranja, ki podeljuje vsakemu uporabniku pravico do rabe, razširjanja in spreminjanja računalniških programov, dokumentov;

jávna prográmska opréma -e -e -e ž *(angl. public domain software)*
programska oprema, katere raba ni omejena z varovanjem materialnih avtorskih pravic; sin. javno programje

lastníška prográmska opréma -e -e -e ž *(angl. proprietary software)*
programska oprema, pri kateri licenčna pogodba omejuje uporabo, spreminjanje ali razširjanje; sin. lastniško programje, zakonsko zaščitena programska oprema; prim. javna programska oprema, odprtokodna programska oprema

licénca -e ž *(angl. licence)*
dovoljenje za uporabo, spreminjanje, razširjanje programske opreme, digitalne vsebine; prim. licenčna pogodba

materiálna ávtorska pravíca -e -e -e ž *(angl. economic right)*
vsaka od avtorskih pravic, ki varuje premoženjska upravičenja nosilca in mu daje izključno pravico nad posameznimi oblikami izkoriščanja avtorskega dela; prim. moralna avtorska pravica

morálna ávtorska pravíca -e -e -e ž *(angl. moral right)*
vsaka od neodtujljivih avtorskih pravic, ki avtorju zagotavlja uresničevanje moralnih interesov v zvezi z avtorskim delom, npr. pravica priznanja avtorstva; prim. materialna avtorska pravica

okŕnjeno prográmje -ega -a s *(angl. crippleware)*
lastniško programje za ogled plačljive, neokrnjene različice, pri katerem je omogočeno omejeno preizkušanje

prôsta prográmska opréma -e -e -e ž *(angl. free software)*
programska oprema, pri kateri licenčna pogodba daje uporabniku pravico uporabe, razširjanja, spreminjanja; sin. odprta programska oprema, odprtokodna programska oprema; prim. lastniška programska oprema, javna programska oprema

zastónjska prográmska opréma -e -e -e ž *(angl. freeware)*
programska oprema, za uporabo katere nosilec materialne avtorske pravice ne zahteva nadomestila, lahko pa postavlja druge omejitve, npr. prepoved spreminjanja, prepoved razširjanja; sin. brezplačna programska oprema, brezplačno programje, zastonjsko programje

Izpitni centri ECDL

ECDL (European Computer Driving License), ki ga v Sloveniji imenujemo evropsko računalniško spričevalo, je standardni program usposabljanja uporabnikov, ki da zaposlenim potrebno znanje za delo s standardnimi računalniškimi programi na informatiziranem delovnem mestu, delodajalcem pa pomeni dokazilo o usposobljenosti. V Evropi je za uvajanje, usposabljanje in nadzor izvajanja ECDL pooblaščena ustanova ECDL Fundation, v Sloveniji pa je kot član CEPIS (Council of European Professional Informatics) to pravico pridobilo Slovensko društvo INFORMATIKA. V državah Evropske unije so pri uvajanju ECDL močno angažirane srednje in visoke šole, aktivni pa so tudi različni vladni resorji. Posebno pomembno je, da velja spričevalo v 148 državah, ki so vključene v program ECDL. Doslej je bilo v svetu v program certificiranja ECDL vključenih že preko 16 milijonov oseb, ki so uspešno opravile preko 80 milijonov izpitov in pridobile ustrezne certificate. V Sloveniji je bilo doslej v program certificiranja ECDL vključenih več kot 18.000 oseb in opravljenih več kot 92.000 izpitov. V Sloveniji sta akreditirana dva izpitna centra ECDL, ki imata izpostave po vsej državi.

AGORA

Micro Team

Znanstveni prispevki

Strokovni prispevki

Pregledni znanstveni prispevki

Informacije

ISSN 1318-1882
9 771318 188001